UNIVERSITY OF CALGARY

Bell state measurements for
quantum communication

by

Venkata Ramana Raju Valivarthi

A THESIS
SUBMITTED TO THE FACULTY OF GRADUATE STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF DOCTOR OF PHILOSOPHY

GRADUATE PROGRAM IN PHYSICS AND ASTRONOMY

CALGARY, ALBERTA
DECEMBER, 2017

Abstract

Over the last few decades, quantum key distribution (QKD) has gained a lot of attention due to its promise of establishing secret keys between authenticated users even in the presence of an eavesdropper who is only confined by the laws of nature. Secure key established by QKD in conjunction with one-time pad (OTP) encryption thus promises to end the long standing battle between code-makers and code-breakers. Spurred by its great promise, QKD has been the first quantum information technology to be commercialized and QKD systems are available from a number of vendors.However, these systems are still vulnerable to side-channel attacks as the components used in these systems don't necessarily conform to the idealistic assumptions made in security proofs of QKD. Of the many components, single photon detectors have been identified as the most vulnerable component allowing, for instance, so-called 'blinding attacks.' In light of this, measurement device independent quantum key distribution (MDIQKD) protocol was proposed as a means to make QKD inherently immune to all possible detector side channel attacks, due to the particular property of the so-called Bell state measurement.

The aim of this thesis is to develop techniques that will allow developing a cost-effective MDIQKD system that is suitable for quantum networks and to use these techniques to perform quantum teleportation on a metropolitan scale for the first time. More precisely this thesis describes the assessment of performance of MDIQKD using different hardware; the development of cost-effective MDIQKD system for quantum networks; the building of a practical quantum random generator (QRNG) suitable for high speed QKD systems; the demonstration of quantum teleportation on a metropolitan scale and the realization of an efficient Bell state analyzer for time-bin qubits that improves the efficiency of all quantum information processing tasks including MDIQKD and quantum teleportation. The above demonstrations constitute an important step towards realizing

practical quantum internet.

Preface

Below is a list of papers that are included in this thesis. Papers are listed according to the order in which they are introduced in Chapter 5 and the Appendix.

1. "Measurement-device-independent quantum key distribution: from idea towards application", Raju Valivarthi, Itzel Lucio-Martinez, Philip Chan, Allison Rubenok, Caleb John, Daniel Korchinski, Cooper Duffin, Francesco Marsili, Varun Verma, Mathew D. Shaw, Jeffrey A. Stern, Sae Woo Nam, Daniel Oblak, Qiang Zhou, Joshua A. Slater and Wolfgang Tittel, Journal of Modern Optics 62, 1141(2015).

2. "A cost-effective measurement-device-independent quantum key distribution system for quantum networks", Raju Valivarthi, Qiang Zhou, Caleb John, Francesco Marsili, Varun B Verma, Matthew D Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Quantum Science and Technology, 2 04LT01.

3. "Practical quantum random number generator based on sampling vacuum fluctuations", Qiang Zhou, Raju Valivarthi, Caleb John and Wolfgang Tittel, arXiv:1703.00559 [quant-ph]

4. "Quantum teleportation across a metropolitan fibre network", Raju Valivarthi, Marcel.li Grimau Puigibert, Qiang Zhou, Gabriel H. Aguilar, Varun B. Verma, Francesco Marsili, Matthew D. Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Nature Photonics,10 67680

5. "Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors", 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, Opt.Express,22, 24497.

Table of Contents

List of Tables

List of Figures and Illustrations

List of Symbols, Abbreviations and Nomenclature

Abbreviation	Definition
QKD	Quantum key distribution
OTP	One-time pad
MDIQKD	Measurement device independent quantum key distribu
DIQKD	Device independent quantum key distribution
QRNG	Quantum random number generator
AWG	Arbitrary waveform generator
FPGA	Field programmable gate array
SG	Signal generator
SNSPD	Superconducting nanowire single photon detectors
APD	Avalanche photodiode
QBER	Quantum bit error rate
SPDC	Spontaneous parametric down conversion
ATT	Attenuator
IM	Intensity modulator
PM	Phase modulator
BSM	Bell-state measurement
SPD	Single photon detector
MZI	Mach-Zehnder interferometer
PC	Polarization controller
PBS	Polarizing beam-splitter
PMBS	Polarization maintaining beam-splitter
HOM	Hong-Ou-Mandel measurement
CLK	Clock

DWDM	Dense wavelength division multiplexing
PD	Photo-detector
QC	Quantum channel
CC	Classical channel
ISO	Isolator
PCB	Printed circuit board
VEDL	Variable electronic delay line
FBG	Fiber-Bragg grating
SHG	Second harmonic generation
PPLN	Periodically poled Lithium Niobate
DM	Dichroic mirror
FP	Fabry-Perot
QST	Quantum state tomography
RF	Radio frequency
LPF	Low pass filter
TTL	Transistor-transistor logic
UMZI	Unbalanced Mach-Zehnder interferometer
UMI	Unbalanced Michelson interferometer
DOF	Degrees of freedom
OAM	Orbital angular momentum

Chapter 1

Introduction

It is fair to say that technologies based on quantum effects such as lasers, transistors etc. have revolutionized human life since the beginning of 20th century [9]. Nevertheless, the full potential of quantum mechanics to enhance existing and foster new technologies is only now beginning to be realized. The push to harness quantum effects for the development of new technologies is, thus, at the forefront of research in a number of groups throughout the world. The aim of this thesis is to develop techniques to control these quantum effects in practical scenarios to be able to bring the technology from the lab to the real world. In particular, it is focused on developing quantum communication technologies.

The thesis is organized as follows. A brief description of the basic components of quantum communication is provided in chapter 2. The role of Bell state measurements in the context of quantum communication is described briefly in chapter 3. Using Bell state measurements to provide secure communication using quantum key distribution is discussed in chapter 4. In chapter 5, a summary of papers included in this thesis is provided along with my contributions to each of the papers. Finally the thesis is concluded in chapter 6, with outlook in chapter 7.

Chapter 2

Background

In the following sections, a brief description of the basic components of quantum communication is provided.

2.1 Qubits

The basic unit of classical information processing, known as the bit, can take values of either '0' or '1'. The two states can be encoded onto different physical systems, e.g, a transistor having a bias current ON or OFF. Similarly the basic unit of quantum information is known as the qubit (short for quantum bit). Unlike the classical bit, it can be in a superposition of the two states '0' and '1'. Mathematically such a superposition can be expressed as $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, where α and β are complex amplitudes and $|\alpha|^2$ ($|\beta|^2$) is the probability of finding the quantum state $|\psi\rangle$ in the state $|0\rangle$ ($|1\rangle$). The possibility of quantum states to exist in these superposition states is one of the main reasons for quantum information processing to have remarkable advantages over the classical counterpart [10].

Single photons, i.e. single excitations of quantized electro-magnetic modes, are typically chosen for transmission of quantum information because of their ability to carry quantum information unperturbed over long distances. In addition, optical fibers have been developed and deployed on a global scale to to send light, or photons over long distances. Currently installed fibers feature a loss of 0.2 dB/km and recently ultra low-loss fibers have been made with loss of about 0.11 dB/km.

Different degrees of freedom of photons such as polarization, time of creation, orbital angular momentum, spatial degree of freedom etc., have been employed to encode quantum information onto photons. Time-bin qubits, exploiting different times of creation of a photon, have been shown to be especially suitable for long distance communication unless otherwise mentioned were used in this thesis [11].

2.2 Preparation and measurement of photonic qubits

Time-bin qubits are typically prepared using either an unbalanced (in the sense of having unequal path lengths) Mach Zehnder interferometer (UMZI) or an unbalanced Michelson interferometer (UMI) in which the photon has an equal probability of taking either the short arm or the long arm. At the interferometer output, the photon emerges in a superposition of having taken both paths, which is equivalent to being in a superposition of two emission times. An alternative method of preparing time-bin qubits is to send a photon with a long coherence time (τ_c) into an amplitude modulator and restrict the presence of the photon wave-packet into two well defined times, i.e, early and late time-bin. A phase inducing element can then be used to impart an arbitrary phase onto one of the time-bins, thus changing the phase difference between early and late. Hence the state is written as $|\psi\rangle = \alpha |e\rangle + e^{i\phi}\beta |l\rangle$, where $|e\rangle$ is the early and $|l\rangle$ the late emission time respectively.

Measurement of qubit (for e.g, $|\psi\rangle$) is done by choosing a measurement basis whose eigen-states are given by $|\phi\rangle \, and \, |\phi^{\perp}\rangle$ (where $|\phi^{\perp}\rangle$ is orthogonal to $|\phi\rangle$). The probability that the state $|\psi\rangle$ ends up in the state $|\phi\rangle$ is given by $| \langle\phi| |\psi\rangle |^2$, which, in other words denotes the overlap between the two states. The measurement of photonic time-bin qubits is typically implemented using a similar UMZI or UMI where the input states are transformed into a superposition of two orthogonal modes and the detection of the photon in one of the modes projects the quantum state of the photon onto the corresponding eigen-state of the measurement setup.

2.3 Entanglement

Photons in addition to being able to exist in superposition states by themselves, can also be entangled with other photons [12]. This puzzling prediction of quantum theory implies that even though the properties of individual photons are completely undefined, the photons behave in tandem as though they are tied together by an invisible string.

A pure bi-partite state (Ψ_{AB}) shared between two parties Alice (A) and Bob (B) is defined to be entangled if the state cannot be written as a tensor product of the states of the individual parties ($|\Psi_A\rangle$ and $|\Psi_B\rangle$), that is

$$|\Psi\rangle_{AB} \neq |\Psi\rangle_A \otimes |\Psi\rangle_B \,. \tag{2.1}$$

It is to be noted that this definition of entanglement can be expanded to any number of parties, who will thus all share the entangled state. Various measures such as tangle, partial positive transpose, concurrence etc., quantify the amount of entanglement. Maximally entangled states refer to the set of states that, for a certain number of parties, maximize the entanglement measures. For bi-partite systems, the maximally entangled states are given in Eqs. 2.2 and are commonly known as Bell states, named after John Bell.

$$\begin{aligned} |\Phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \\ |\Psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \end{aligned} \tag{2.2}$$

Entangled states are at the heart of many quantum communication tasks such as quantum teleportation, entanglement swapping, superdense coding, etc. and also for quantum computing [10]. Quantum entanglement has also been shown to be useful to establish symmetric secure keys between authenticated users, which then can be used to communicate in secrecy even assuming an eavesdropper with arbitrary computational power [13].

Photonic quantum entanglement is typically generated using non-linear processes such as spontaneous parametric down-conversion (SPDC) in non centro-symmetric crystals and more recently by emission from solid-state systems. Entangled photons can be created using different DOFs of photons such as polarization [14], time-bin [15], OAM [16], frequency [17], energy-time [18] etc. Entanglement between hybrid species such as between atoms and photons has also been reported [19]. This is crucial to long distance quantum communication using quantum repeaters.

2.4 Bell state measurement

Bell state measurements (BSMs) are essential for many quantum communication protocols such as quantum teleportation [20], entanglement swapping [21], super-dense coding [22], quantum repeaters [23], some quantum key distribution protocols [24, 25], and also in quantum information processing tasks such as linear optics quantum computing [26].

A BSM is defined as the projection of two qubits onto one of the four maximally entangled Bell states, shown in Eqs. 2.2. Hence, the BSM is sometimes also referred to as an entangling measurement. A photonic Bell state measurement is typically implemented using a beam splitter followed by measurement devices that are able to identify two orthogonal modes in the chosen degree of freedom for qubit encoding. Common Bell state measurement setups for time-bin qubits and polarization qubits are shown in Fig. 2.1. Such photonic Bell state measurements mainly rely on the principle of two-photon interference, also known as Hong-Ou Mandel (HOM) interference described below.

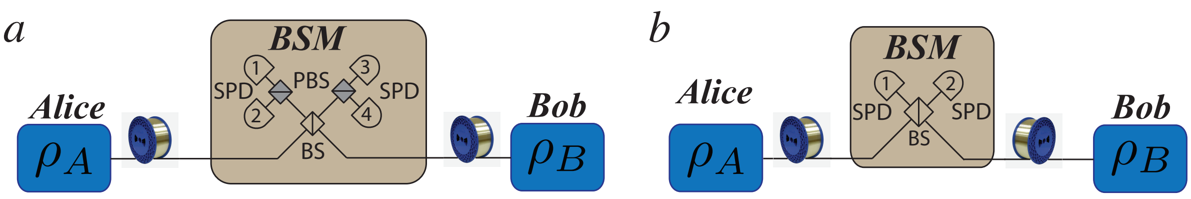


Figure 2.1: Part a shows the BSM setup for polarization qubits. Here the polarization qubits prepared by Alice and Bob impinge on a beam splitter after traveling through independent links. The two outputs of the beamsplitter each include a polarization beam splitter followed by two single photon detectors and hence allow identifying the two orthogonal polarization modes. Part b shows the BSM setup for time-bin qubits, where the outputs of the beam splitter are detected directly using single photon detectors (SPDs) which should be able to identify early and late temporal modes. Figure taken from [1]

2.4.1 HOM interference

The setup for measuring HOM interference is similar to that for the BSM, shown in Fig. 2.1. Given two indistinguishable single photon Fock states are at the beam-splitter (BS) input, the photonic state following the beam-splitter transformation is:

$$\begin{aligned} |1\rangle_1 \otimes |1\rangle_2 \implies & \frac{1}{4}(i\,|1\rangle_3 + |1\rangle_4) \otimes (|1\rangle_3 + i\,|1\rangle_4). \\ = & \frac{1}{2} i\,|1\rangle_3\,|1\rangle_3 + i\,|1\rangle_4\,|1\rangle_4 \,. \end{aligned} \tag{2.3}$$

As seen in Eq. 2.3, quantum interference prohibits photons from taking separate paths and the photons bunch in the same but a random output port of the BS. The quantum interference only occurs if the input photons are completely indistinguishable. Varying the distinguishability between the two photons (for e.g. the arrival time difference), the number of photons detected in coincidence between the two detectors at the output of the BS changes from a maximum value (max) at largest distinguishability to a minimum value (min) at largest indistinguishability. This dip in coincidences with increasing indistinguishability shown in Fig. 2.2 for the temporal domain is known as the HOM dip.

The visibility (V) of the dip is given by

$$V = \frac{(max - min)}{max}. \tag{2.4}$$

With pure single photons at the input, the visibility reaches a maximum of 100%, assuming no noise from the detectors, i.e. dark counts. The visibility varies with the photon number distribution of the photon sources at the input, the indistinguishability of the sources, noise in the detectors etc. For the commonly used coherent sources, which create a Poissonian photon number distribution, the theoretical maximum for the visibility is 50% and for thermal sources, the theoretical maximum is 33%. Hence, the visibility is typically used to quantify the indistingushability of modes from sources with known photon number distributions.

2.4.2 Photonic BSM

As mentioned, a typical photonic BSM setup consists of a beam-splitter followed by detectors. The input and output spatial modes are labelled 1,2 and 3,4, respectively. The four Bell states mentioned in Eq. 2.2, after undergoing the beam-splitter transformation, become

$$\begin{aligned}
|\Phi^{\pm}\rangle_{12} &= \frac{1}{\sqrt{2}}(|00\rangle_{12} \pm |11\rangle_{12}) \\
&\implies \frac{i}{2}(|00\rangle_{33} + |00\rangle_{44} \pm |11\rangle_{33} \pm |11\rangle_{44}) \\
|\Psi^{+}\rangle_{12} &= \frac{1}{\sqrt{2}}(|01\rangle_{12} + |10\rangle_{12}) \\
&\implies \frac{i}{\sqrt{2}}(|01\rangle_{33} + |01\rangle_{44}) \\
|\Psi^{-}\rangle_{12} &= \frac{1}{\sqrt{2}}(|01\rangle_{12} - |10\rangle_{12}) \\
&\implies \frac{1}{\sqrt{2}}(|10\rangle_{34} - |01\rangle_{34})
\end{aligned} \tag{2.5}$$

From Eq. 2.5, we can see that a coincidence of photons in modes 0 and 1 in the

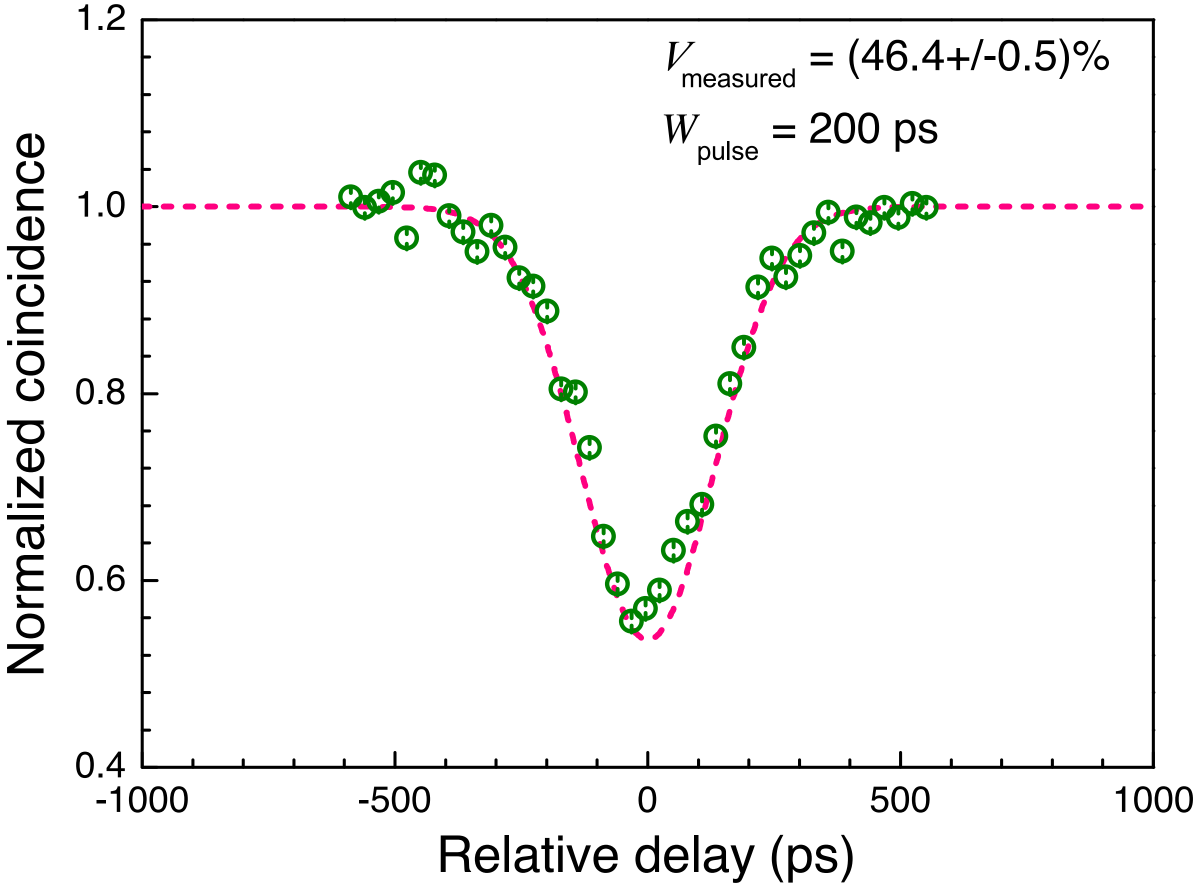


Figure 2.2: The figure shows the dip in coincidences with varying distinguishability (here, the arrival time of two photons on the beam splitter) between the two photons. The visibility of the dip is close to 50%, as photon sources with Poissonian photon number distribution are used. Figure taken from [2]

same output port of the beam-splitter signals projection onto $|\Psi^+\rangle$ and a coincidence of photons in modes 0 and 1 in different output ports of the beam-splitter is a signature of $|\Psi^-\rangle$. Also, it is evident that coincidences of photons in modes 0 or 1 in the same output of the beam-splitter cannot distinguish between states $|\Phi^+\rangle$ and $|\Phi^-\rangle$. So with the above set-up we can unambiguously distinguish 2 of the 4 Bell states.

2.4.3 Efficiency of photonic BSM with linear optics

As seen from Eq. 2.5, two of the four Bell states can be detected unambiguously and hence the theoretical limit of the efficiency for the setup in Fig. 2.1 is 50%. In fact, it has been proven that with linear optics and no auxiliary photons, the efficiency of the BSM is limited to 50% [27]. Various proposals have been made to improve the efficiency of a BSM using just linear optics but with additional auxiliary photons [28]. According to that proposal the efficiency scales with the number of auxiliary photons, $2^N - 2$, as $1-1/2^N$. Thus an infinite number of additional photons is required to reach the efficiency of 100%.

A conceptually simple way to improve the efficiency of the BSM to 100% is to implement a $CNOT$ (short for controlled not) gate using non-linear optics. The transformation of the four Bell states under a $CNOT$ is given in Eq. 2.6.

$$\begin{aligned} CNOT\,|\Phi^{\pm}\rangle &= |\pm\rangle\,|0\rangle \\ CNOT\,|\Psi^{\pm}\rangle &= |\pm\rangle\,|1\rangle\,, \end{aligned} \tag{2.6}$$

where $|\pm\rangle = \frac{1}{\sqrt{(2)}}(|0\rangle \pm |1\rangle)$

While an efficient implementation of a $CNOT$ gate with photons remains elusive [29, 30], such a gate has been well demonstrated in several atomic and stationary qubit systems [31, 32]. However, the transfer of a qubit from a traveling photon to e.g, a microwave qubit, the most widely pursued quantum information processing platform, requires a quantum transducer [33, 34], which has yet to be demonstrated.

Chapter 3

Bell state measurements for quantum communication

Quantum communication is the art of sending quantum information from one location to another [35]. BSMs are an integral part of many quantum communication primitives, and it is vital for protocols such as quantum teleportation [20], entanglement swapping [21], super-dense coding [22] and quantum repeaters [23], as described below.

3.1 Quantum teleportation

Quantum teleportation allows for the transfer of quantum states from one system to another without them ever interacting with each other, i.e, a disembodied transfer of a quantum state from one system to another. The fascinating thing about quantum teleportation is the ability to transfer quantum states between sytems separated by arbitrarily long distances, as long as the entangled state is shared between the parties involved. Quantum teleportation of states between photons is the focus of this thesis, but teleportation of quantum states between hybrid species such as atoms and photons has also been demonstrated. Recent advances in teleportation is briefly reviewed in [36].

The protocol we shall use is presented in the figure 3.1. Alice prepares the qubit ($|\psi\rangle_A = \alpha\,|0\rangle_A + \beta\,|1\rangle_A$) to be teleported at location A and sends it to Charlie at location C. Bob prepares an entangled pair (for e.g, $|\Phi^+_{BC}\rangle$) and sends one member of his entangled state to location C. Charlie, after receiving both states, performs a BSM, as described in section 2.4.1. This results in the qubit state of Alice to be teleported to the other member of entangled state at location B, modulo a unitary transformation. More precisely this

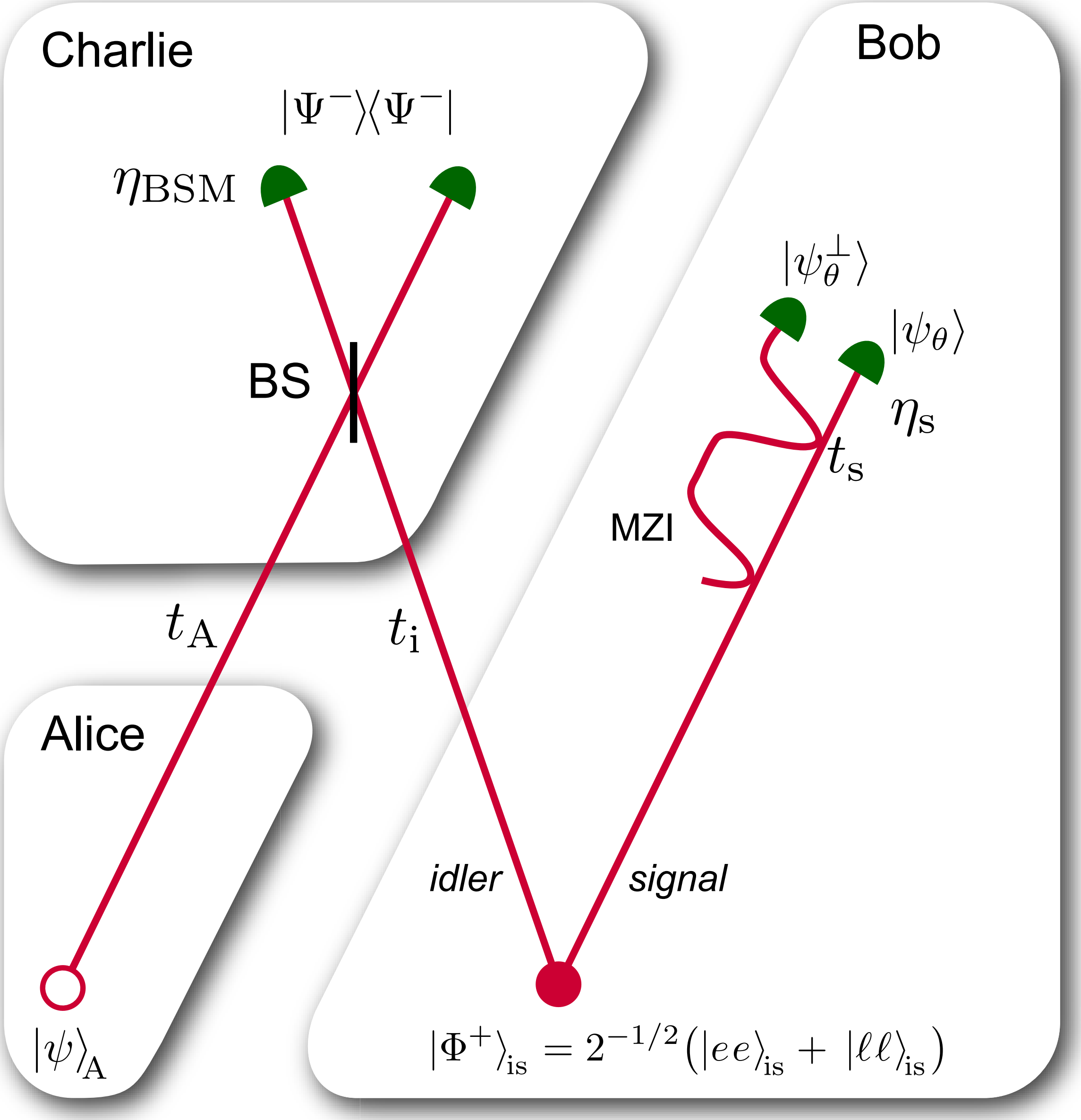

Charlie
$|\Psi^-\rangle\langle\Psi^-|$
η_{BSM}
BS
Bob
$|\psi_\theta^\perp\rangle$
$|\psi_\theta\rangle$
η_{s}
t_{s}
MZI
t_{A}
t_{i}
Alice
idler
signal
$|\psi\rangle_{\mathrm{A}}$
$|\Phi^+\rangle_{\mathrm{is}} = 2^{-1/2}(|ee\rangle_{\mathrm{is}} + |\ell\ell\rangle_{\mathrm{is}})$

Figure 3.1: Teleportation scheme for time-bin qubits. Alice prepares the qubit to be teleported $|\psi_A\rangle$ and sends the qubit to Charlie through a channel with transmission t_A. Bob prepares an entangled state $|\Phi^+_{is}\rangle$ and sends one of the two photons through an independent channel to Charlie with transmission t_i. Charlie performs a BSM with efficiency η_{BSM} (in this instance only onto $|\Psi^-\rangle$). Bob applies the necessary unitary transformation on the *signal* photon (in this instance σ_Y) using a MZI to recover Alice's qubit. Figure taken from [3]

is described mathematically as shown in Eq. 3.1 below.

$$\begin{aligned}
\left|\psi\right\rangle_A \otimes \left|\Phi^+\right\rangle_{BC} &= (\alpha\left|0\right\rangle_A + \beta\left|1\right\rangle_A) \otimes (\frac{1}{\sqrt{2}}(\left|00\right\rangle_{BC} + \left|11\right\rangle_{BC})) \\
&= \left|\Phi^+\right\rangle_{AC} \otimes (\alpha\left|0\right\rangle_B + \beta\left|1\right\rangle_B) + \left|\Phi^-\right\rangle_{AC} \otimes (\alpha\left|0\right\rangle_B - \beta\left|1\right\rangle_B) + \\
&\left|\Psi^+\right\rangle_{AC} \otimes (\alpha\left|1\right\rangle_B + \beta\left|0\right\rangle_B) + \left|\Psi^-\right\rangle_{AC} \otimes (\alpha\left|1\right\rangle_B - \beta\left|0\right\rangle_B) \\
&= \left|\Phi^+\right\rangle_{AC} \otimes (I\left|\psi\right\rangle_B) + \left|\Phi^-\right\rangle_{AC} \otimes (\sigma_Z\left|\psi\right\rangle_B) + \left|\Psi^+\right\rangle_{AC} \otimes (\sigma_X\left|\psi\right\rangle_B) + \\
&\left|\Psi^-\right\rangle_{AC} \otimes (\sigma_Z\sigma_X\left|\psi\right\rangle_B)
\end{aligned} \tag{3.1}$$

It is important to note that Bob's state has four equally probable terms. Hence, without the information of whether the BSM was successful and the result of the BSM, the quantum state of the second member of the entangled state, which remained with Bob, is in a completely mixed state. As a consequence, the result of Charlie's BSM must be communicated to Bob for him to be able to apply the correct unitary transformation and recover Alice's original qubit. It is to be noted that this necessity of communication of the BSM result prevents any form of instantaneous communication as a consequence of quantum teleportation.

3.2 Entanglement swapping

Entanglement swapping allows entangling two quantum systems that have never interacted before. Due to the protocol's close relation to quantum teleportation, it is often referred to as teleportation of entanglement.

For entanglement swapping, Alice prepares an entangled pair, for e.g. in state $\left|\Phi^+\right\rangle_{AC_1}$ and sends the C_1 member of the pair to Charlie. Bob also prepares an entangled state, for e.g, $\left|\Phi^+\right\rangle_{BC_2}$ and sends the C_2 member of the pair to Charlie. Once Charlie receives both members, one from Alice and one from Bob, he performs a BSM on them. If the

BSM is successful, entanglement is swapped to particles A and B, which are with Alice and Bob, respectively. This is mathematically shown in the equation below.

$$
\begin{aligned}
|\Phi^{+}\rangle_{AC_1} \otimes |\Phi^{+}\rangle_{BC_2} &= \frac{1}{\sqrt{2}}(|00\rangle_{AC_1} + |11\rangle_{AC_1}) \otimes \frac{1}{\sqrt{2}}(|00\rangle_{BC_2} + |11\rangle_{BC_2}) \\
&= |\Phi^{+}\rangle_{AB} \otimes |\Phi^{+}_{C_1C_2}\rangle + |\Phi^{-}\rangle_{AB} \otimes |\Phi^{-}_{C_1C_2}\rangle + |\Psi^{+}\rangle_{AB} \otimes |\Psi^{+}_{C_1C_2}\rangle + \\
&\quad |\Psi^{-}\rangle_{AB} \otimes |\Psi^{-}_{C_1C_2}\rangle
\end{aligned} \tag{3.2}
$$

As in the case of teleportation, Charlie needs to communicate the result of the BSM to Alice or Bob or both to recover the swapped entanglement. Without the BSM information, the joint state of Alice's and Bob's particles is completely mixed.

3.3 Superdense coding

Superdense coding allows two bits of information to be communicated by exchanging just one qubit. The protocol is described below. Suppose the two parties, Alice and Bob, share an entangled state, for e.g. $|\Phi^{+}\rangle_{AB}$. Alice chooses to apply one of the four unitaries $I, \sigma_X, \sigma_Z, \sigma_Y$ corresponding to two bits of information of 00,01,10,11. These operations transform the initial entangled state shared between Alice and Bob, $|\Phi^{+}\rangle_{AB}$, to $|\Phi^{+}\rangle_{AB}$, $|\Psi^{+}\rangle_{AB}$, $|\Phi^{-}\rangle_{AB}$, or $|\Psi^{-}\rangle_{AB}$. After applying the unitary, Alice sends her part of the entangled state to Bob and Bob can recover the two bits of information by performing a BSM.

3.4 Quantum repeaters

Quantum communication suffers from the long standing problem of loss during the transmission of quantum information. Photons, best suited for carrying quantum information over long distances, are transmitted from one location to another using optical fibres or free-space links. Standard optical fibres have loss of 0.2 dB/km at telecommunication wavelengths, and state-of-the-art ultra low loss fibres have about 0.11 dB/km. To give an example of the impact of such loss, for inter-continental distances ($\sim$ 2000 km), photons will experience loss of about 220 dB, which is to say that for every 10^{22} photons sent, only one photon makes it at the end on average. In classical communication, this problem is overcome by the use of classical repeaters. In essence, the total link is divided into smaller sub links and the light is amplified using Erbium doped fiber amplifiers (EDFA) after each sub-link such that there is sufficient receiving power for error-free communication at the end of each sub-link.

Unfortunately, in the case of quantum communication, for e.g, the distribution of quantum entanglement, amplification is not possible because of the no-cloning theorem [37]. The no-cloning theorem prohibits creating two or more perfect copies of an unknown quantum state. In addition to experiencing loss, quantum information may also decohere during the transmission. In this context, decoherence is any effect that scrambles the quantum information without annihilating the actual photon. Thus, decoherence can make quantum communication intractable. As a solution to this problem, quantum repeaters based on various principles have been proposed and research by groups across the globe is underway. A classification of different repeater types/architectures based on their ways of overcoming loss and decoherence is presented in [38]. Our group is focused on developing quantum repeaters based on entanglement generation using photon pair sources and absorptive quantum memories, as described below.

As discussed in section 3.2, entanglement swapping is the teleportation of entanglement between two particles that have never interacted. The total desired distance of quantum communication, L is divided into N sub-links, or elementary links, each of length $l = \mathrm{L/N}$. Heralded entanglement is generated between the ends of each elementary link and stored in quantum memories. One way to do that is to perform entanglement swapping where a BSM at the centre of each elementary link heralds the successful generation of entanglement between the stored photons at the ends of each elementary link. The BSM result in each elementary link must be communicated to the ends of the link to recover the entanglement as mentioned in section 3.2. Note that all the elementary links may not have generated heralded entanglement at the same time, as photons' transmission though each lossy elementary link is a probabilistic process. However, the quantum memories allow buffering of entanglement across an elementary link until the entanglement has also been distributed through the neighboring elementary link. Another entanglement swapping procedure then allows creating entanglement across the two links. This procedure is repeated until the entanglement is generated at the ends of the total link.

It is to be noted that quantum communication using free space channels is also an active research field. Quantum repeaters using satellites are also being investigated by various research groups [39]. The recent demonstration of the distribution of quantum entanglement using a satellite over a distance upto 1200 km not only promises secure communication over such long distances, but also helps us to deepen our understanding of quantum effects over such macroscopic scales [40].

3.5 Summary

In summary, BSMs play a pivotal role in realizing future quantum communication networks. All the techniques developed during the course of this thesis work will go a long way to help building real world quantum networks.

Chapter 4

Bell state measurements for quantum cryptography

4.1 Cryptography

Cryptography (Greek for ‘secret writing’) is the study and practice of sending secret messages from one party (user) to another [41]. Typically the parties (users) are referred to as Alice and Bob. Secret communication is one of the basic necessities on which modern society is based upon. Cryptography has evolved over the years from the use of primitive ‘substitution’ cipher during the times of Julius Caesar to the present modern cryptography, which relies on complex mathematical theory and computer science. While human beings have gradually gotten better at keeping messages secret from third parties, it is fair to say they have gotten equally good at cracking (known as code-breaking or hacking) secret messages. Edgar Allan Poe, an American writer and an amateur cryptographer, wrote “... it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve ...”. It is desired that the two parties are able to exchange secret messages without making any assumptions about the computational abilities of an eavesdropper who is potentially listening to this exchange. This is sometimes referred to as ‘unconditional security’ or ‘information-theoretic security’. Fortunately, Claude Shannon proposed in [42] a simple encryption method, known as one-time pad (OTP), which achieves secure communication with information-theoretic security.

4.2 One-time pad

Alice and Bob are assumed to share a random cryptographic key unknown to any third party. Alice uses this key to encrypt the message that she wants to send it to Bob. The encryption is done by simply XORing the message bitwise with the key. The encrypted message, known as ciphertext, is sent to Bob using a public channel. Bob, using the same random key, decrypts the message by simply XORing the ciphertext with the key bitwise and thus recovering the original message. Any third party who doesn't have the key sees a scrambled message and can only guess the message.

4.2.1 Security of one-time pad encryption

Let K,x,y denote the possible values for a cryptographic key, message and ciphertext, respectively. Let's assume n be the total length of the message, x. Thus the lengths of K and y are also n. Since K needs to be random among all the possible values,

$$Pr[K] = 2^{-n} \tag{4.1}$$

where Pr[A] denotes the apriori probability that A occurs. Now, the conditional probability that a ciphertext occurs given a message

$$Pr[y|x] = Pr[K = x \oplus y] = 2^{-n}. \tag{4.2}$$

Also,

$$Pr[y] = \sum_{x \in 2^{-n}} Pr[x] \times Pr[y|x] = \sum_{x \in 2^{-n}} Pr[x] \times 2^{-n} = 2^{-n}. \tag{4.3}$$

The probability that a message occurs, given a ciphertext,

$$Pr[x|y] = \frac{Pr[y|x] \times Pr[x]}{Pr[y]} = Pr[x]. \tag{4.4}$$

Thus every message is equally likely to occur even though the cipher text is known. Since no assumptions were made on the computational abilities of the eavesdropper, the OTP encryption provides perfect secrecy. The problem of secure communication is now reduced to the problem of exchanging secret keys in the presence of an eavesdropper. But techniques based on classical physics have not been able to achieve key distribution between remote users without making assumptions about computational abilities of an eavesdropper.

Let's assume, Alice and Bob share two magical coins which, when tossed, somehow give the same value ('heads' or 'tails', corresponding to bit values of 0 or 1). Alice and Bob can now toss this coin n times and generate a key. They can now use the OTP to start exchanging secret messages. And if somehow we can make these magical coins, it would seem that secret communication can be achieved. But it is to be noted that this doesn't rule out the possibility of an eavesdropper also having a magical coin which gives the same toss as the coins of Alice and Bob. Thus we can never be sure that the coins with the above mentioned properties don't have a copy, which in principle, can be with an eavesdropper.

Present day secure communication is therefore done by making some assumptions on the eavesdropper, mainly the computational abilities.

4.3 Public key cryptography

Modern day cryptography heavily relies on public key cryptography, also known as asymmetric key cryptography. Different keys are used to encrypt and decrypt the messages (unlike the OTP encryption discussed in section 4.2), hence the name. Every user has two keys, known as public key and private key. As the names suggest, the public key is known to everyone, whereas the private key is only known to the user. Alice uses Bob's public key to encrypt a message and sends the ciphertext over a public channel. Only Bob, who has the private key corresponding to the public key used by Alice, will be able to decrypt the message. Also, unlike in OTP encryption, the key can be used more than once and thus reduces the overhead of generating fresh keys every time. The main assumption here is that the private key cannot be computed once the public key is known. Although various proposals have been made to realize public key cryptography, the most commonly used today is based on the RSA algorithm named after its inventors Ronald Rivest, Adi Shamir, and Len Adleman [43].

4.3.1 RSA

RSA is based on the assumption that prime factoring of a large number n is practically difficult. The public key is based on the large prime number n and the private key is based on the two prime factors of n. The best known classical algorithms for prime-factoring scale exponentially with n and hence to negate the possible increasing computational power of an eavesdropper, it was enough to increase the size of the number n. But Peter Shor proposed an algorithm that solves prime factoring in polynomial amount of time but using quantum computational resources [44]. If a quantum computer of the required scale is built, our present day RSA crypto systems will be easily broken, which will have dire consequences.

4.4 Post-quantum cryptography

Since the advent of Shor's algorithm, intensive research has been going on to build crypto systems that are resilient to a quantum computer. These algorithms are known as post-quantum algorithms [45] and examples include lattice based cryptography [46], isogeny based elliptic curves [47] etc. It is important to note that there have been no definitive proofs that the best known algorithms to solve the above mentioned problems cannot be improved upon. Moreover the security that can be achieved using the above algorithms is still computational security, that is the eavesdropper is assumed to be bounded to having limited computational power. And hence an eavesdropper could store current ciphertexts and decipher them once he/she has enough computational power in the future, which might have some very serious consequences. Thus crypto systems which are able to provide unconditional security are greatly desired.

4.5 Quantum key distribution

Although quantum computers seem like a disruptive technology, quantum mechanics provides a way of achieving information theoretic security by allowing two remote users to exchange keys even in the presence of an eavesdropper. “ The quantum taketh and the quantum giveth.” Quantum key distribution (QKD) is easily the most mature quantum technology today. Since the first proposal of QKD in 1984 by Charles Bennett and Gilles Brassard [48], intensive research has been going on on both theoretical and experimental fronts to build systems achieving information-theoretic security [49–55], and commercial QKD systems are available for purchase now [5].

4.6 BB84

BB84, named after its inventors, is the first proposal that helped start the now rich field of quantum cryptography. The security of BB84 relies on Heisenberg’s uncertainty principle, which says that there exist complementary observables and knowing full information about one observable prevents obtaining any information about the other observable. The steps of the most commonly implemented version of BB84 are discussed below:

4.6.1 Qubit transmission and mesasurement

Alice prepares qubits randomly in the eigen-states of σ_Z and σ_X bases i.e. in $(\left|0\right\rangle, \left|1\right\rangle)$ and $(\left|+\right\rangle, \left|-\right\rangle)$, respectively, with probability p_Z and p_X. These states are sometimes referred to as BB84 states. The states $\left|0\right\rangle, \left|+\right\rangle$ correspond to bit ‘0’ and the states

$|1\rangle, |-\rangle$ correspond to bit '1'. Photons are typically employed to encode the qubits and then sent using optical fibres or free-space channels to Bob. Bob chooses to measure the received qubits randomly in the Z-basis and in the X-basis with probabilities p_Z and p_X respectively, and keeps the corresponding bit values of his measurement results.

4.6.2 Basis reconciliation

Alice and Bob use a public authenticated channel to broadcast their basis choices of preparations and measurements respectively. They discard all the bits where they have a basis mismatch. The left-over key is referred to as the sifted key.

4.6.3 Parameter estimation

At this point, ideally Bob's measurement results exactly match with what Alice had prepared earlier. However, any imperfections during the preparation or measurement of qubits, decoherence during channel transmission or an eavesdropper trying to gain information about the qubits sent by Alice will cause some mismatch between the bits recorded by Alice and Bob. They use a public-authenticated channel to reveal a randomly selected subset of their bits in the X basis. The ratio of the number of mismatched bits to the total number of bits in the subset is known as quantum bit error rate (QBER) and is denoted as e^X. If the QBER is below a certain threshold, they go ahead with the next step. Otherwise, they abort the protocol here and start over from step one. This QBER is essentially used to quantify and bound the information gained by an eavesdropper during the qubit transmission.

4.6.4 Error-correction

A classical error-correction procedure is employed by Alice and Bob to correct the errors in the Z-basis. All the additional bits of information that are exchanged through this process are also assumed to be known to an eavesdropper. By the end of this procedure, the bits of Alice and Bob, created and measured in the Z-basis are identical with a very high probability.

4.6.5 Privacy amplification

Now the eavesdropper's information (quantified during parameter estimation step) is removed by privacy amplification. Typically, 2-universal hash functions are used to compress the key, thereby reducing the information of an eavesdropper about the key close to zero.

4.6.6 Key rate

The final key rate that can be achieved at the end of the protocol is given by

$$S \geq Q^Z(1 - h_2(E^X)) - fQ^Z h_2(E^Z) \tag{4.5}$$

where Q refers to the gain (the probability to obtain a detection per qubit after transmission through the channel), h_2 the binary entropy, E the QBER, f the efficiency of the error-correction procedure employed, and the superscript indicates the basis for which the quantities are calculated. As can be seen from the key-rate formula, the second quantity $Q^Z h_2(E^X)$ indicates the eavesdropper's information about the raw key while the third quantity $fQ^Z h_2(E^Z)$ indicates the total bits exchanged in the public channel during error-correction. The final key is only known to the authenticated users and they can use the OTP as mentioned above to communicate with information-theoretic security.

4.7 Figures of merit

Figures of merit for a practical QKD system are the final achievable key rate, the longest distance over which QKD is possible and the ease with which the system can be built, which will ultimately effect its long-term stability and reliability. In the following sections, the main components of a QKD system such as sources to prepare qubits, the channels through which the qubits are sent and the detectors to finally measure the qubits are briefly discussed.

The above mentioned protocol assumes single photon sources to prepare the required qubits. The closest systems to achieve single photon sources are heralded photon sources based on spontaneous parametric down conversion (SPDC) [57, 58], quantum dots, and colour centres such as Nitrogen vacancies (NV) [59] and Silicon vacancies (SiV) [60]. While tremendous progress has been made in the development of the above mentioned sources, they are still not considered to be practical because of their low rates, lack of indistinguishability or requirement of cryogenic temperatures. Instead, most of the demonstrations of QKD are done using phase randomized coherent states with low mean photon number, which mimic single photon sources.

4.8 Phase-randomized coherent states

Phase-randomized coherent states are mixed states in photon number space with Poissonian distribution as shown below. Coherent state α is given by

$$|\alpha\rangle = e^{\frac{-|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n}} |n\rangle \tag{4.6}$$

After phase-randomization

$$\begin{aligned}\frac{1}{2\pi}\int_0^{2\pi} ||\alpha|e^{i\theta}\rangle \langle|\alpha|e^{i\theta}|\, d\theta \\ &= \frac{1}{2\pi}\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}\frac{|\alpha|^{m+n}}{\sqrt{mn}}\,|n\rangle\langle m|\int_0^{\infty} e^{i(m-n)\theta}d\theta \\ &= \sum_{n=0}^{\infty} e^{-\mu}\frac{\mu^n}{n!}\,|n\rangle\langle n|\end{aligned} \tag{4.7}$$

where $\mu = |\alpha|^2$ is the mean photon number per emitted light pulse.

The probability that n photons are emitted from this source is thus given by,

$$P(n) = e^{-\mu}\frac{\mu^n}{n!} \tag{4.8}$$

As seen from eq. 4.7, with a low mean photon number the probability that n photons are emitted goes down exponentially with n. So, whenever a source emits something other than vacuum, it is a single photon with very high probability. And such sources are readily available, as they are just laser pulses attenuated to the single-photon level ($\mu \ll 1$). This helped in numerous demonstrations of QKD in various settings.

4.9 Quantum channel

In QKD experiments, it is assumed that eavesdropper has full control over the channel. As mentioned in section 2.1, optical fibres or free space channels are typically used for the transmission of optical qubits. The transmission profiles of standard single mode fiber and atmosphere for different wavelengths is shown in Figure 4.1. Thus, when using standard single mode-fibres, light sources to prepare qubits and single photon detectors (SPDs) to measure qubits at telecommunication wavelengths are desired. Also, this presents an opportunity to take advantage of currently developed devices for classical

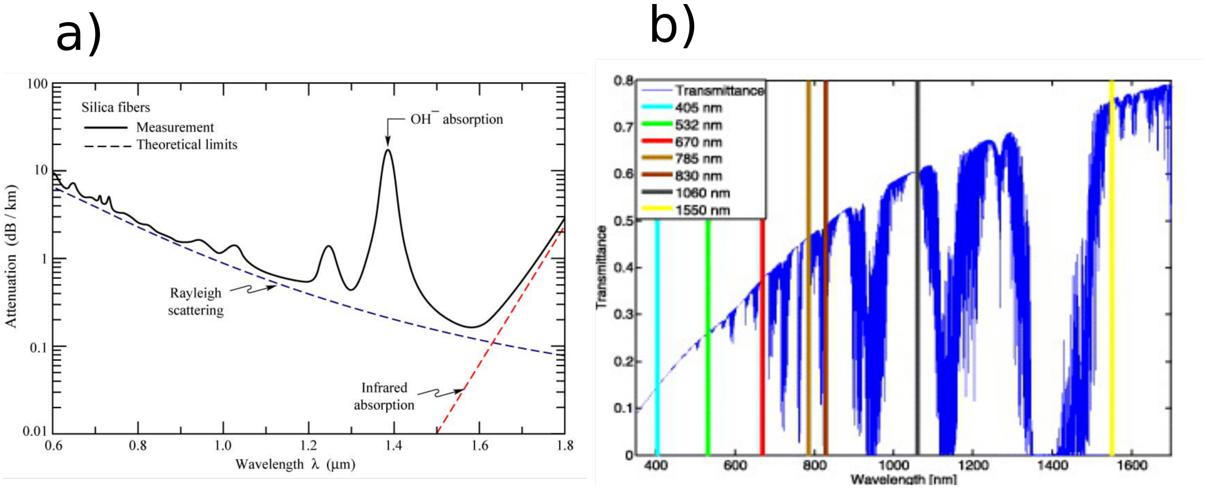


Figure 4.1: Part a shows the attenuation of optical fiber versus wavelength. Present telecommunication infrastructure is based on wavelengths around 1550 nm. Part b shows the transmission of light in atmosphere versus wavelength. Best choice of wavelength is based on the transmission, availibility of single photon sources and detectors, diffraction etc., Refer to [4]

tele-communication and adapt them for QKD devices. For free-space channels, sources and detectors which are compatible with light of wavelengths close to 800 nm can also be used. It is to be noted that even in the absence of an eavesdropper, these channels can be depolarizing due to the presence of stray light, chromatic dispersion, polarization mode dispersion etc. Necessary measures have to be taken to mitigate these effects and obtain key at the end.

4.10 Single photon detectors

It is fair to say that single-photon detector (SPD) technology had a direct impact on the development of QKD systems as is evident from the rise of number of publications in quantum cryptography since the development of SPDs. The SPDs used for this thesis, avalanche photo detectors (APDs) and superconducting nanowire SPDs (SNSPDs), are described below.

4.10.1 Avalanche photo detectors

Avalanche photo detectors are semi-conductor devices that are able to detect individual photons [61]. They are p-n junction diodes reverse biased above and below the breakdown voltage as shown in Figure 4.2. This is called gating the detector. When the bias voltage is above the breakdown voltage, it results in a high electric field in the depletion region. When a photon hits the active area or a thermal excitation occurs (leading to false clicks, known as dark counts) during this time, this results in the creation of an electron-hole pair with the two charge carriers moving with high velocities in opposite directions. In turn, this creates more electron hole pairs and thus turns into an avalanche, generating a detectable macroscopic current, then converted to a voltage signal by passing it through a resistor. The rising edge of this voltage signal signifies the arrival time of the photon. This current is then actively quenched by reducing the bias voltage below the breakdown voltage. Some electron hole pairs are not completely quenched and thus have a non-zero probability of resulting in a dark count in the coming gate cycles. This is called after-pulsing. Usually the detectors are cooled used thermo-electric coolers (TECs) to ∼223 K to reduce dark counts.

APDs based on InGaAs (Indium Gallium Arsenide) and Si (Silicon) are available to detect light at single photon level at ∼ 1500 nm and ∼ 800 nm wavelengths. Commercial APDs are available now with gate rates as high as GHz, efficiency as high as 30% [62] for 1550 nm and dark counts close to 25 Hz [63]. These characteristics have a direct impact on the performance of a QKD system, i.e. the final key rate and the longest distance at which non-zero key can be obtained.

4.10.2 Superconducting nano-wire single photon detectors

Superconducting nanowire single photon detectors (SNSPDs) operate on a different principle as opposed to APDs [64]. As the name suggests, nano wires made of superconducting

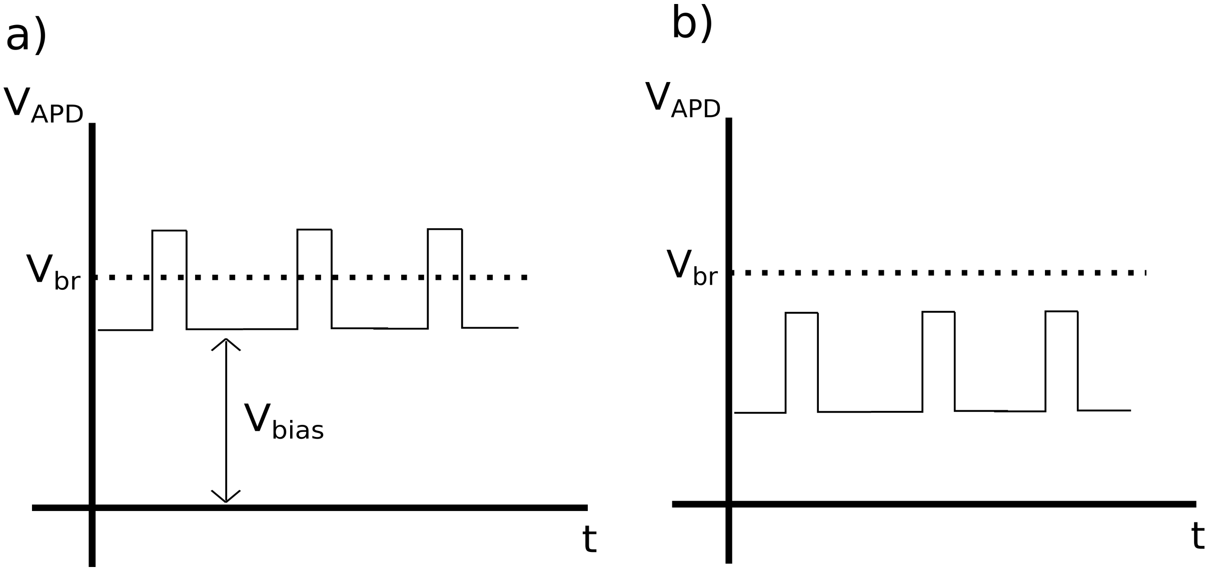


Figure 4.2: Part a shows the APD biased above and below the breakdown voltage, known as gating. The APD is sensitive to light at the single photon level when the bias is above the breakdown voltage. Part b shows that upon shining bright light, the voltage across the APD is lowered below the breakdown voltage at all times and thus the APD becomes insensitive to single photons.

material such as Tungsten Silicide (WSi) are current biased below the critical current. When a photon or light at single photon level hits the wires, it creates a ‘hot spot’, where the material is not super-conducting anymore. This forces the current to flow around the hot spot thereby creating a current density exceeding the superconducting critical current density. This results in a detectable resistance across the detector, which is used to signify the presence of photon. Unlike APDs, SNSPDs are inherently free running and thus need not be gated. Also, they boast high efficiencies ($\sim 93\%$) and few dark counts (~ 50 Hz) [65]. The only downside to the SNSPD, if any, is the requirement of cryogenic temperatures (< 4 K) to be able to operate them.

The development of SNSPD not only led to improved performances of QKD systems but also some ground-breaking results such as loophole-free violations of Bell inequalities, which is discussed briefly in section 4.12.

All the above mentioned devices, if they deviate from their ideal behaviour, may open avenues for an eavesdropper to exploit and thereby gain more information about the key without leaving much of a trace. These deviations lead to side-channel attacks as described below.

4.11 Side-channel attacks

Real-world devices rarely conform to the idealistic assumptions made in theoretical proofs. These deviations could in principle be exploited by an eavesdropper as shown by different research groups using various QKD demonstrations. This active research field is known as quantum hacking [5, 7, 66–75]. Some well known attacks on sources and detectors of QKD systems are described below.

4.11.1 Quantum hacking of sources

4.11.2 Trojan horse attack

As shown in Figure 4.3, an eavesdropper can inject strong light into Alice's system, used to prepare qubits. Typically, modulators, be it amplitude or polarization modulators are employed to prepare different qubit states. If some of the strong light is leaked to these devices, the effect of the modulators is imprinted on the light sent from the eavesdropper. In principle, this could be at a different wavelength to the one used by Alice's source. By analyzing the light that is reflected, the eavesdropper can in principle obtain full information about the states prepared by Alice and thus obtaining full information about the key.

Detailed counter measures to prevent Trojan horse attacks are presented in [76]. By using an isolator that only allows light in one direction and by adding appropriate filters, Alice can prevent an eavesdropper, Eve, sending such strong light into the system. Also monitoring incoming light with a power-meter could reveal the presence of an eavesdropper.

4.11.3 Photon number splitting attack

Although, never demonstrated experimentally, photon number splitting (PNS) attack represents one of the most sophisticated quantum hacking methods [66]. As mentioned in section 4.8, when ideal single photon sources are not used to prepare qubits, there is a non-zero probability of emitting multiple photons. Eve could in principle perform a quantum non-demolition measurement (QND) [77, 78] on the photon number of the pulses sent by Alice without disturbing the qubit state encoded onto photons. For multi photon events, she stores one of the photons in a quantum memory and sends the rest to Bob. For single photon events, she simply blocks the transmission as she has full control of the quantum channel. The total detection events at Bob's station could be

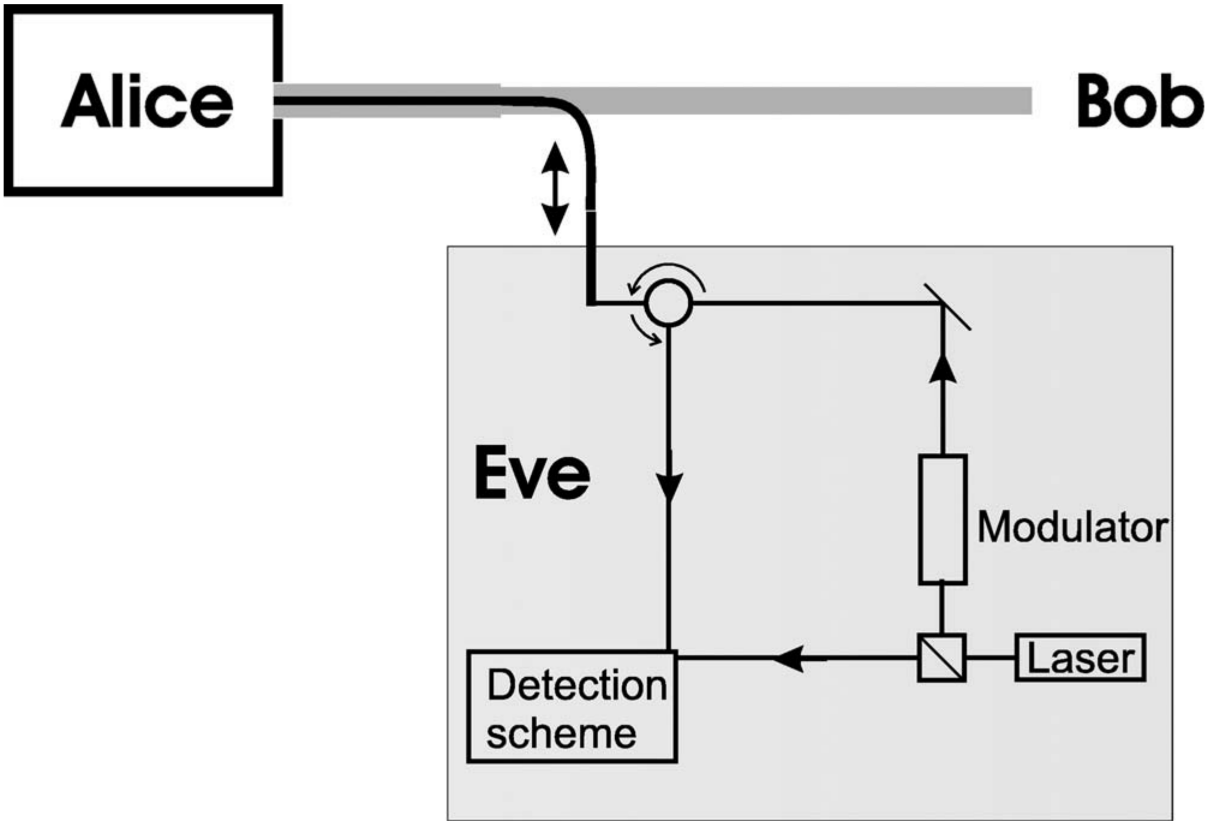


Figure 4.3: Eve occupies part of the quantum channel and tries to gain information about Alice's qubits by injecting light into Alice's station. Eve compares the modulated light reflected from Alice's station with un modulated light using a suitable detection scheme. Figure taken from [5].

made the same as the ones without the attack by controlling the channel loss. Since Bob receives the quantum state untouched, no trace of eavesdropping is seen during the parameter-estimation step. Hence, when calculating the secret key rate the photon number distribution of the emitted light needs to be taken into account in calculating the secret key rate. This leads to very low key rates or very short distributable distances when using attenuated laser pulses.

Fortunately, decoy state method was proposed using which the fraction of detection events emanating from single photons can be estimated without making any assumptions on the quantum channel, as described below.

4.11.4 Decoy state method

The decoy state method allows Alice and Bob to estimate detections and errors coming from single photon emissions [6,24,79–81]. For this, Alice, in addition to preparing qubit states, randomly changes the mean photon number of the laser pulses between different values$(\mu, \nu, o ...)$. Different mean photon numbers have different probabilities of emitting different number states as shown in Eq. 4.8. But for a given number state, the behaviour of the quantum channel must be the same, irrespective of the mean photon number of the source. This is the essence of the decoy state method. An infinite number of intensities, or mean-photon numbers, are required to exactly estimate the detection events coming from single photon events. Fortunately it was later shown that just with a total of three mean photon numbers [79], the gains of single photon events can be estimated very close to the actual value as shown below:

$$Q_\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu} \tag{4.9}$$

where Q_μ denotes the probability of having a detection at Bob when Alice prepares attenuated laser pulses with mean photon number μ, and Y_n denotes the probability of having a detection at Bob when Alice sends n photons into the channel.

Similarly for mean photon numbers ν_1 and ν_2 we have,

$$Q_{\nu_1} = \sum_{i=0}^{\infty} Y_i \frac{{\nu_1}^i}{i!} e^{-\nu_1} \tag{4.10}$$

$$Q_{\nu_2} = \sum_{i=0}^{\infty} Y_i \frac{{\nu_2}^i}{i!} e^{-\nu_2} \tag{4.11}$$

Notice that Y_n is the same for all the mean photon numbers μ, ν_1 and ν_2. From equations 4.10 and 4.11, the terms Y_0 and Y_2 are eliminated and a lower bound on Y_1 is calculated with the formula shown below:

$$Y_1 \geq \frac{\mu}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2} \Big[Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2} \big(Q_\mu e^\mu - max(\frac{\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1}}{\nu_1 - \nu_2}, 0) \big) \Big] \tag{4.12}$$

A similar strategy is followed to calculate an upper bound for the error-rate for single photons. The final key rate shown in Eq.4.5 is modified for sources that have non-zero multi photon probability. It is given by:

$$S \geq Q_1^Z (1 - h_2(E_1^X)) - Q_\mu^Z f h_2(E_\mu^Z) \tag{4.13}$$

where Q indicates gains and e error-rates. The subscripts ’1’ and μ indicate quantities pertaining to single photons and pulses with mean photon number μ, respectively, and superscripts indicate the basis.

The difference in the secret key rates with and without applying decoy states method is shown in Fig. 4.4. As can be seen from the figure, there are significant improvements in both the key rates and the longest distance over which secret key can be extracted.

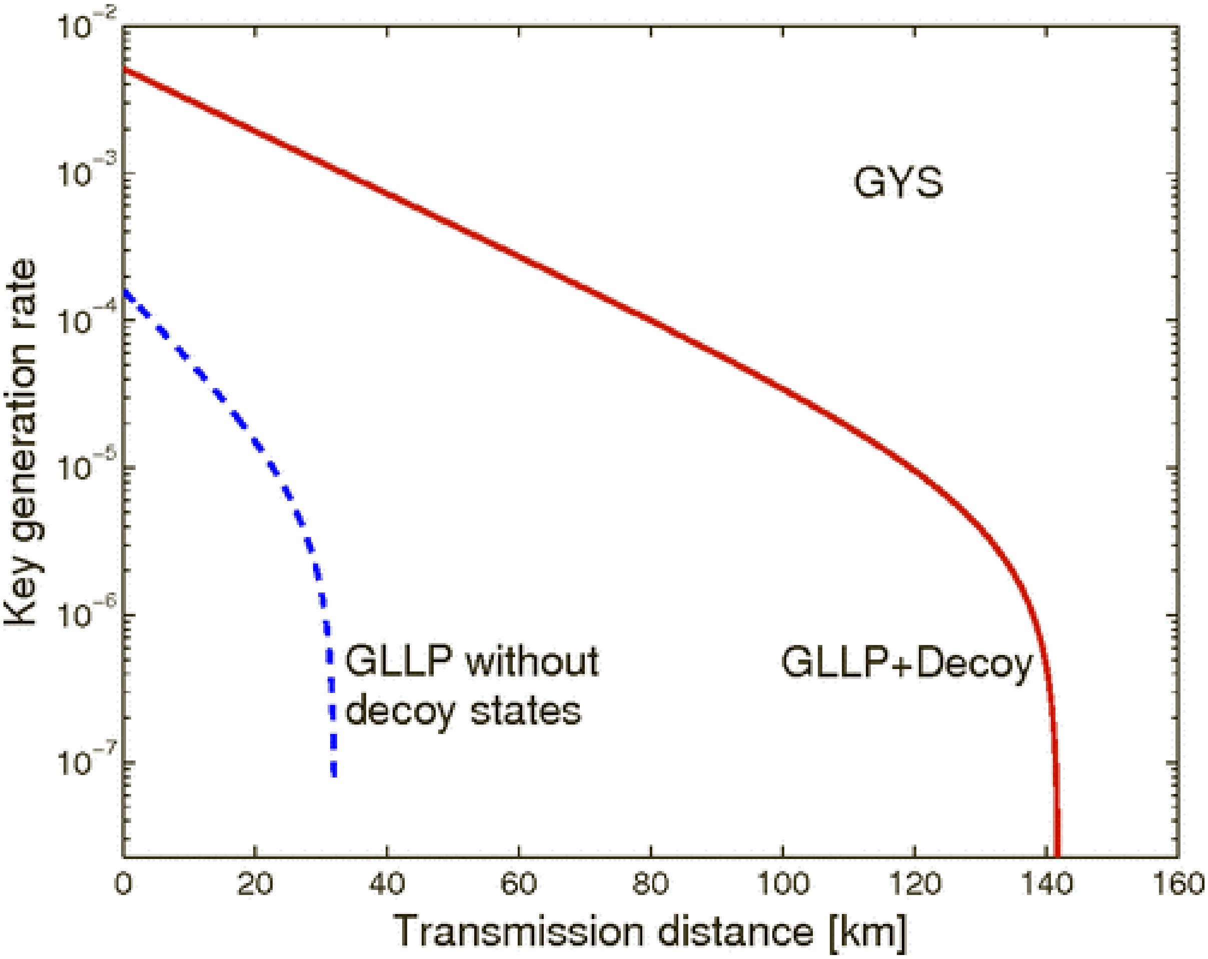


Figure 4.4: Key rate comparison with and without applying the decoy states. GLLP, named after it's authors Gottesman, Lo, Lu$\ddot{t}$kenhaus and Preskill, denotes the secure keyrate from the security proof. The parameters for the simulation of the keyrate vs distance is taken from the experiment done by Gobby, Yuan and Shields (GYS). Figure taken from [6].

4.11.5 Quantum hacking of detectors

Numerous successful attacks that have been performed on single photon detectors clearly show that they are the most vulnerable components of QKD systems. One of the key reasons for this is that unlike Alice, Bob needs to allow light (single photons), coming from Alice, into his station and thereby opens an avenue for an eavesdropper to perform sophisticated attacks on his single photon detectors. As discussed in section 4.11.2, Alice can simply block the light coming from the quantum channel using isolators and necessary optical filters as no light is expected to come from the other direction. One of the most well-known attacks on detectors is discussed below:

4.11.6 Blinding attack

This is an attack demonstrated, by *Lydersen et al* [7], where an eavesdropper, by shining bright light onto Bob's detectors, can completely remote control the detectors and thus gain all information about the key without leaving any trace. As discussed in section 4.10.1, avalanche photo diodes are biased above breakdown voltage to be sensitive to light at the single-photon level. When high intensity-light is incident upon the detector, the bias voltage is reduced and remains permanently below the breakdown voltage. Thus the detector is no longer sensitive to single photons; it is 'blinded'. But one can still get 'clicks' from the detectors when an additional pulse of light of sufficient intensity is incident on the blinded detector. Thus, an eavesdropper can remotely control when the detector clicks or not by controlling the intensity of the light incident on Bob's detector.

To get the information about the key, *Lydersen et al* performed the so called intercept-resend attack. This is an attack where the eavesdropper intercepts Alice's signal, processes the signal and sends a new signal based on the result onto Bob. As Alice is sending qubits randomly, the eavesdropper randomly measures the qubits in different bases just like Bob. Based on the result obtained, she sends a bright pulse whose intensity is tai-

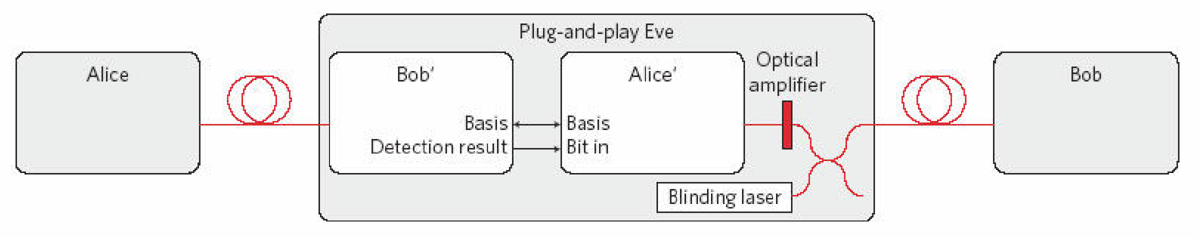


Figure 4.5: Eve occupies the quantum channel and intercepts Alice's qubits. She measures the qubits just like Bob would and then prepares strong pulses light with state according to the measurement result. She then sends the pulses to Bob's detectors which have been previously blinded. The intensity of state dependent light is adjusted so that Bob's detectors click only when he chooses the same measurement basis as Eve. Figure taken from [7]

.

lored in such a way that Bob will get a click only when he chooses the same basis as the eavesdropper. In all the other cases, i.e. if there is a basis mismatch, there is no click and the event is hence discarded during post-processing. Thus the eavesdropper and Bob have the same bits and no extra error is introduced because of the eavesdropping. The attack is summarized in figure 4.5. The attack has been shown to be working with SNSPDs too [82].

Various measures have been proposed to detect the attack, e.g, putting a detector at Bob to monitor spikes in classical power. Some sophisticated measures include changing the design of the electrical circuits used in the detector or randomly changing the quantum efficiency of the detector [83, 84].

To summarize, deviations in the devices from assumptions made in the QKD protocols (inherent or made by an eavesdropper) lead to possibilities of side-channel attacks. One way to overcome this problem is to develop counter measures for each attack. But it is still possible that in the future, an eavesdropper can come up with a more sophisticated attack which might render the deployed QKD systems insecure. The other way to overcome this problem is to devise protocols where minimal assumptions are made on the devices used in QKD.

One such protocol is known as device independent quantum key distribution (DIQKD) where key is secured by measuring statistics of the detections with no assumptions made on the inner workings of the devices used. This rather strong form of security [25,85–87] is discussed in the section below.

4.12 DIQKD

The essence of DIQKD is discussed in simple arguments by Renner et al, in [88], and briefly summarized below. Following the discussion in section 4.2, if Alice and Bob had magical coins which give the same result when flipped, it doesn't exclude the possibility of an eavesdropper having a magic coin whose results are also exactly correlated with those of Alice and Bob.

Now let's assume Alice and Bob instead have two magical coins whose coin toss results are labelled A_1, A_2 and B_1, B_2 respectively. Alice and Bob can only toss one coin at a given time. Let's impose the condition,

$$A_1 = B_1, B_1 = A_2, A_2 = B_2, B_2 \neq A_1 \tag{4.14}$$

Assigning either '0' or '1' to any of the coins obviously doesn't satisfy at least one of the equalities. But since only one of the coins can be tossed at a time, there is no contradiction. If we assume Alice tossed both the coins at the same time and if they gave the same result, Bob must have tossed B_1 and in the other case, Bob must have tossed B_2. This simple contradiction forces Bob to toss a particular coin and thus deprives him of freedom of choice. And the same argument also prevents any external party to have a clone of one of the coins A_1 or A_2. Because, if such a clone exists (for e.g, $Z = A_1$) and when Z and A_2 are tossed together, it prevents Bob from having a freedom of choice of tossing a coin. This shows that such correlations described in eq. 4.14 are monogamous and cannot be cloned. On the other hand, if we assume that nature doesn't allow any freedom of choice or in other words if everything is pre-determined, the notion of cryptography is meaningless.

Now to get a key, Alice and Bob randomly choose one of the coins and toss. They publicly communicate the choice of the coins and get the key from the results of the coin tosses. The remarkable thing is that the coins could be manufactured by an untrusted third party and Alice and Bob just have to verify the condition in eq. 4.14 by choosing a random subset of their tosses.

While quantum mechanics allows stronger correlations than classical mechanics, it doesn't allow us to build exactly the strong correlations described in Eq. 4.14. Nonetheless, we can get close. The quantum correlations between particles are often quantified by the amount of violation of a Bell's inequality. The most commonly used version of Bell's inequality known as CHSH Bell inequality [89] (named after its inventors Clauser, Horne, Shimony, Holt) is shown in Eq. 4.15.

$$S = |E(a,b) + E(a,b') + E(a',b) - E(a',b')| \leq 2 \tag{4.15}$$

where a, a' and b, b' represent the choices of measurements that can be made by Alice and Bob respectively. $E(a,b) = \frac{C(a^1,b^1)+C(a^{-1},b^{-1})-C(a^1,b^{-1})-C(a^{-1},b^1)}{C(a^1,b^1)+C(a^{-1},b^{-1})+C(a^1,b^{-1})+C(a^{-1},b^1)}$ is the correlation coefficient. $C(a^x, b^y)$ denote the coincidences when Alice and Bob choose measurement settings a and b and get measurement results x and y respectively. When described by local realistic theories, the maximum value that the S-parameter can attain is 2. Any violation of the inequality indicates that the correlations cannot be described by a local hidden variable theory and thus can be considered truly non-local. Quantum mechanics predicts correlations using which we can obtain the value of S parameter defined in

Eq. 4.15 as high as $2\sqrt{2}$.

Experimentally an entangled state (for e.g, $|\Phi^{+}\rangle_{AB}$) is prepared and one member per entangled pair is distributed to Alice and Bob. Alice randomly chooses to make a measurement of the particle in the σ_Z or σ_X basis, and Bob randomly chooses to make a measurement of his particle in the $\frac{\sigma_Z+\sigma_X}{2}$, $\frac{\sigma_Z-\sigma_X}{2}$ or σ_Z basis. Alice and Bob get key when they both choose the measurement basis σ_Z. The S parameter is calculated with the measurement choices of Alice and the first two choices for Bob. The deviation of the S parameter from $2\sqrt{2}$ is used to quantify the information leaked to the eavesdropper, which is later removed by privacy amplification. The key-rate, taken from [87], is given by,

$$r \geq 1 - h(E) - h(\frac{1+\sqrt{(\frac{S}{2})^2-1}}{2}) \tag{4.16}$$

where E represents the QBER and S is defined in Eq. 4.15. One needs to be careful when calculating the violation of Bell-inequality [90]. Two main loopholes have been identified that need to be closed to discard the possibility of correlations that can be described using local hidden variables. They are known as 'locality' loophole and 'detection' or 'fair-sampling' loophole, and are briefly described below.

4.12.1 Locality loophole

To close the locality loophole, the two stations of Alice and Bob need to be space like separated during the measurement. This is to rule out the possibility that any signal moving at the speed of the light or less can communicate the choice of basis from one station to another. Also, the source has to be space-like separated from both the stations of Alice and Bob.

4.12.2 Fair-sampling loophole

To close the fair-sampling loophole, at least $\sim 83\%$ or $\sim 67\%$ of the total possible detection signals need to be sampled based on the chosen Bell inequality [91,92]. This is to avoid the possibility of detection results only showing the favourable results to violate the inequality. The above-mentioned efficiencies include the transmission losses and also the detection efficiencies of the detectors employed.

Closing both loopholes simultaneously and thus performing a 'loophole free Bell inequality' experiment has eluded the scientific community for a long time. Fortunately, with the development of necessary technology, different groups have demonstrated loophole free violations of Bell inequalities in different settings and also using different physical entities [93–96]. It is to be noted that the first loophole free Bell inequality experiment have used two entangled sources combined with a BSM in the middle to create event-ready entanglement between spins in diamond that were located far enough apart. This further verifies the importance of being able to perform BSM with photons coming from independent sources.

Even though this predicts a promising future of DIQKD, this protocol is still considered to be impractical at this time because of considerably low key rates and rather demanding requirements on the efficiencies of signal detection. This reduces the maximum possible distance over which DIQKD is possible to a few km. Proposals have been made to extend the distance of DIQKD, but an experimental demonstration of DIQKD is yet to be reported [97].

Therefore, instead of trying to avoid all possible side-channel attacks, some QKD protocols only focus on attacks against the most vulnerable components of the QKD systems, i.e. SPDs. All known attacks on the sources can be prevented by simple measures, as discussed in section 4.11.1.

4.13 Measurement device independent QKD

To overcome the hacking attacks proposed and demonstrated on SPDs, two approaches may be pursued. One is to come up with strategies to overcome the known attacks through improved technology including technology that allows monitoring if attacks take place. As mentioned earlier, all possible attacks on the SPDs might not be known at this point of time and also it is still possible for an eavesdropper to develop techniques that circumvent the countermeasure. The other approach is to come up with a protocol that is inherently immune to all-known and yet-to-be discovered attacks on the the SPDs. One such protocol is measurement device independent quantum key distribution (MDIQKD) [24]; it is inspired by time-reversed entanglement generation [98, 99]. The protocol is described below:

4.13.1 MDIQKD protocol

Unlike in the BB84 protocol, Alice and Bob both prepare qubits randomly in one of the four BB84 states ($|0\rangle, |1\rangle, |+\rangle, |-\rangle$), corresponding to bits (0,1,0,1) and send them to Charlie through independent channels. Charlie, who can in principle be an eavesdropper, has the full control of the SPDs. Charlie, after receiving the qubits from Alice and Bob is supposed to perform a BSM. For the security of the protocol, it is to be noted that a projection onto just one of the Bell states is sufficient, but being able to perform a BSM onto more than one Bell state will have the advantage of increased key rates. Charlie publicly announces which of the qubits resulted in a successful BSM and also the result of the BSM. Alice and Bob throw away the bits where the BSM was unsuccessful, and Alice flips her bits based on the result of the BSM (for e.g. $|\Psi^-\rangle$). They repeat the procedure until they have enough successful BSM signals [100]. Then Alice and Bob use a publicly authenticated channel to check the basis in which they prepared the qubits and discard the bits with mismatched basis. They calculate the error-rate in the X-basis to assess the information leaked to an eavesdropper, and then they perform error-correction and finally privacy amplification to get the final key. The final key rate, S, is given by:

$$S \geq Q^Z(1 - h_2(E^X)) - Q^Z f h_2(E^Z) \tag{4.17}$$

where Q refers to the gain, the probability for a BSM, E refers to the error-rate, h_2 to the binary entropy and f to the efficiency of the error-correction procedure employed. The superscripts indicate the basis of the corresponding quantity.

The above protocol assumes using single photon sources, which, as mentioned above, are not quite practical. So, attenuated laser pulses are used instead and the PNS attack is avoided by using decoy-states from which gains and error-rates pertaining to single photons are estimated efficiently. Accordingly, the key rate is modified to:

$$S \geq Q^Z_{11}(1 - h_2(E^X_{11})) - Q^Z_{\mu\nu} f h_2(E^Z_{\mu\nu}) \tag{4.18}$$

where the subscripts 11 indicate the value for gains and error-rates stemming from single photons coming from Alice and Bob and $\mu\nu$ indicate the value for gains and error-rates when Alice uses a mean photon number μ and Bob uses a mean photon number ν.

4.13.2 Security and measurement device independence

The security of MDIQKD and measurement device independence can be intuitively understood from the concepts of monogamy of entanglement [101] and entanglement swapping. Monogamy of entanglement shows that the correlations cannot be arbitrarily shared between large number of qubits. If two systems share maximal correlations, i.e. if they are maximally entangled, then a third system cannot be correlated at all with the two. Alice and Bob preparing qubits randomly in one of the BB84 states is equivalent to them having each prepared a Bell state and randomly measured one member of the pairs in the X or Z basis. An eavesdropper would not see in both cases any difference between the two scenarios as he/she would see completely mixed states coming from Alice's and Bob's station. When qubits reach Charlie, he can either perform a BSM using the SPDs, or any other measurement. When he performs a BSM, the entanglement is swapped to the qubits at Alice's and Bob's stations, ideally resulting in a maximally entangled state. This can be verified by Alice and Bob by examining a random subset of their results. Any other measurement from Charlie, deviating from a BSM, will not result in maximal entanglement between Alice's and Bob's qubits, thereby revealing the malice of Charlie. Thus, no assumptions need to be made about the SPDs used in the QKD system, or more generally the measurement devices, making it resistant to any known or future to be discovered attacks on the SPDs.

4.13.3 Error-rate in X-basis

When attenuated laser pulses are used to prepare qubits, error-rates $\geq 25\%$ are seen when qubits are prepared in the X-basis. Hence Z-basis is used to extract the key while the X-basis is used to calculate the leakage of information about the key to an eavesdropper. The large error-rates in the X-basis are due to the fact that multi-photon emissions lead to spurious BSMs whereas multi-photon emissions in the Z-basis don't.

4.13.4 Challenges with practical implementation

Although MDIQKD has the advantage of resistance to detector attacks, it has the added challenge of performing a BSM on qubits traveling through independent channels. Due to the dynamic properties of real-world fiber links, the polarization and arrival time of photons change, potentially making them completely distinguishable. As mentioned in section 2.4.1, this prevents one from performing the BSM. This prevented experimentalists for many years to implement a BSM in a real-world setting. Our group developed sufficient feedback mechanisms to overcome this hurdle and thus implement BSM outside the laboratory [102]. This seminal demonstration spurred more experimental research and furthermore led to improvements of the performance of the MDIQKD protocol [62, 103–116].

4.13.5 Advantages of MDIQKD

In addition to being immune to all detector-based attacks, MDIQKD is particularly suitable for star-type networks, in which one Charlie, holding all the expensive equipment, can connect a large number of simple users (See figure 4.6). Cost-effective star networks based on MDIQKD can be built by placing all the expensive components of the QKD systems at the central station and making all the sources simple. Also, MDIQKD can be seamlessly upgraded (not disruptively replaced) to future quantum repeater networks, which share the BSM with MDIQKD.

To summarize, MDIQKD, which is based on BSMs, renders quantum hacking of detectors obsolete and only sources are left for quantum hackers to focus on. Also, MDIQKD can be seen as a stepping stone for star-type networks.Furthermore development of MDIQKD benefits the development of quantum repeaters, which will finally provide secure communication over continental distances.

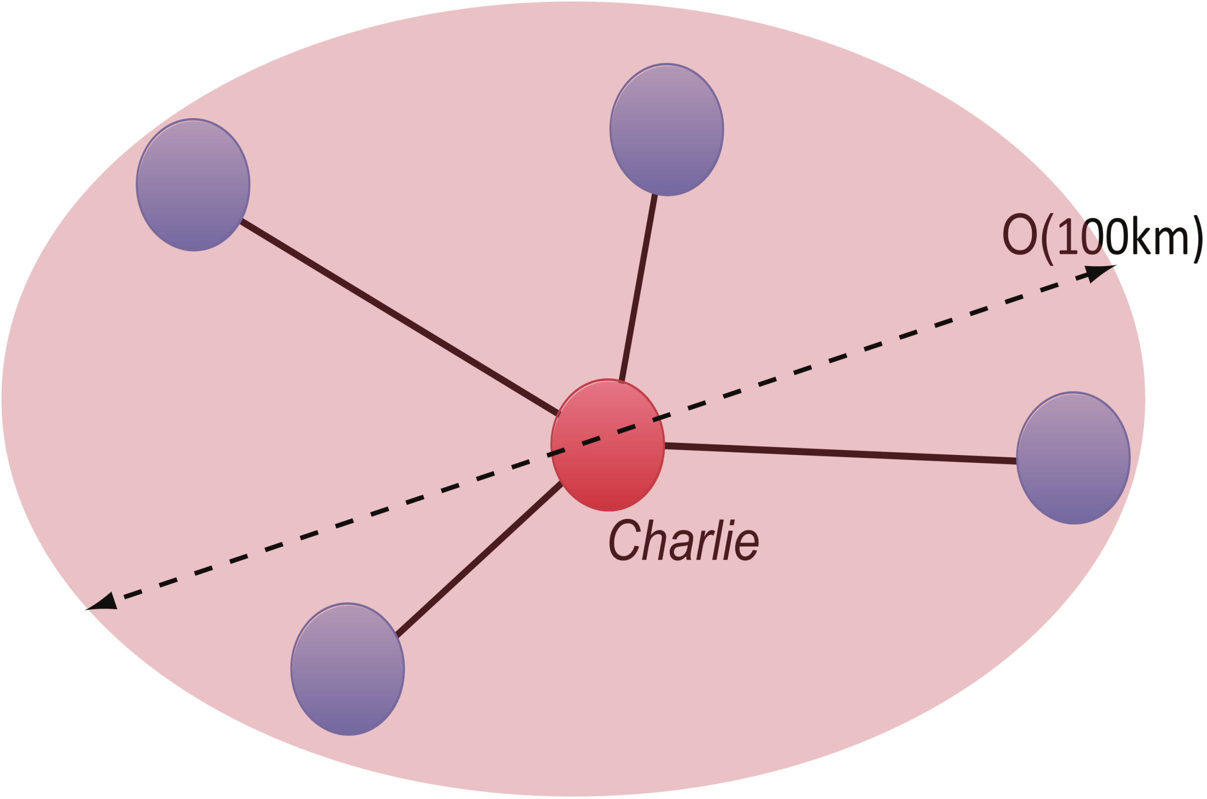


Figure 4.6: A star-type network where several users are connected to Charlie located at the center. The diameter of the network can be extended to a few hundred kilometers, even without the use of a quantum repeater [3, 8].

Chapter 5

This thesis

The aim of this chapter is to briefly summarize and discuss my contributions to each of the papers mentioned in the Appendix to this thesis. These papers comprise my thesis work.

My PhD thesis was concerned with the development of robust BSMs and their use in several quantum communication protocols such as MDIQKD and quantum teleportation. These demonstrations pave the way to a real world quantum repeater which is the ultimate aim of our research group.

5.1 Papers

5.1.1 Paper I

In this paper, we analyze the performance of MDIQKD using different qubit preparation hardware such as expensive and bulky signal generators and field programmable gate array (FPGA) based homemade signal generators, different SPDs such as InGaAs detectors and SNSPDs, and different quantum channels such as fiber spools and real world fiber links. We find that FPGA-based signal generators do not compromise the quality of the generated qubits and that employed feedback mechanisms help to operate the MDIQKD system in real-world environments. SNSPDs offer the best performance in terms of key rates and distance over which MDIQKD is possible. Finally we demonstrate that MDIQKD is possible with channel loss of up to 60 dB, which corresponds to 300 km of optical fiber (assuming loss of 0.2 dB/km).

My contributions to this work include developing the experimental setup and taking *measurements for configurations 3,4 and 5. I also contributed to writing the parts of manuscript concerning configurations 3,4 and 5.*

5.1.2 Paper II

In this paper, we develop our initial proof-of-principle demonstration system to a full running QKD system with the ability of random preparation of qubits and decoy states. We develop a time-tagging module which tags the qubit settings at Alice and Bob which resulted in a successful BSM at Charlie. We developed feedback mechanisms which are inherently free-running which aids in higher key rates for MDIQKD. And all the expensive components such as the SNSPDs and feedback mechanisms are with Charlie, which help in a future cost-effective implementation of a MDIQKD network.

My contributions to this work include co-developing the optical setup, taking measurements with Qiang Zhou, analyzing the results, co-writing manuscript with Qiang Zhou and Wolfgang Tittel and partly dealing with the referee's comments for the final publication.

5.1.3 Paper III

In this paper, we develop a practical quantum random number generator (QRNG) based on sampling vacuum fluctuations. Unlike the typically-used pseudo-random number generators (PRNG) in QKD systems, QRNGs do not require an initial random seed and its randomness is derived from a process that is inherently random. In our QRNG, we use the property of phases of laser pulses being random when switched on and off from below lasing threshold. The random phases are then converted to random intensity fluctuations by interfering the pulses with another laser at the same wavelength. The demonstration of integrability of our QRNG with our MDIQKD system is left for future demonstrations.

My contributions to this work include helping Qiang Zhou with developing the experi-

mental setup and taking measurements and also editing the manuscript to be suitable for publication.

5.1.4 Paper IV

In this paper, we demonstrate quantum teleportation at a metropolitan scale for the first time. We develop a new notion of teleportation distance, which is the distance (as the bird flies) between the BSM and the photon that receives the teleported qubit, at the time of BSM. We report a record teleportation distance of 6.2 km. Also, by extending the technique of decoy states to quantum teleportation, we calculate the fidelity of single qubit teleportation, which allowed us to truly claim the quantumness of the teleportation. Our demonstration establishes an important requirement for quantum repeater-based communications and constitutes a milestone towards a global quantum internet.

My contributions to this work co-developing the experimental setup of Alice's qubit preparation, co-developing the necessary feedback mechanisms, extending the decoy state technique to quantum teleportation, taking measurements, analyzing and interpreting the results and writing parts of manuscript.

5.1.5 Paper V

In this paper, we improve the efficiency of the BSM employing time-bin qubits. While a coincidence detection of *early* and *late* temporal modes in different detectors implies the detection of $|\Psi^-\rangle$, a coincidence detection of *early* and *late* temporal modes in the same detector implies the detection of $|\Psi^+\rangle$. Since the traditionally used InGaAs SPDs have a deadtime of 1 μs, BSM of $|\Psi^+\rangle$ was never demonstrated experimentally using time-bin qubits. Here, by employing SNSPDs that have a deadtime of only 50 ns, we demonstrate the BSM of both $|\Psi^-\rangle$ and $|\Psi^+\rangle$. This helped us to increase the BSM efficiency to 29.5 %, which is a $\sim$30 fold increase compared to previous demonstrations.

My contributions to this work include changing the setup to be suitable for both the Bell state measurements, taking the measurements, analyzing and interpreting the results, and co-editing the manuscript for final publication.

Chapter 6

Conclusion

To conclude, the ability to perform BSMs robustly is pivotal for several quantum communication protocols such as MDIQKD and teleportation.

During this thesis, a QKD system that is immune to all detector based hacking has been developed. Time-bin qubits, which are shown to be ideal for long distance quantum communication have been employed. The performance of the MDIQKD system was assessed using different hardware such as different qubit preparation hardware, different SPDs such as APD-based SPDs and the recently developed SNSPDs. SNSPDs, which have extremely low noise and high detection efficiencies have facilitated extracting key at 60 dB loss, which is equivalent to having 300 km of standard optical fiber between Alice and Bob.

This assessment helped us to build a fully automated MDIQKD system based on FPGAs, which allows random preparation of qubits and intensities. Feedback mechanisms which are inherently free running and that can be operated from Charlie have been developed without the need of any extra SPDs. The simplistic nature of the sources used to perform MDIQKD can be taken advantage of in star type networks, where all the expensive components are placed at a central station. Furthermore, QRNG based on sampling vacuum fluctuations has been developed; it is ready to be integrated with our MDIQKD system. This avoids the use of pseudo-RNG which would be a potential bottle neck for practical security of QKD systems.

By performing BSM on photons traveling through independent channels, quantum teleportation has been demonstrated for the first time at a metropolitan scale. The decoy state technique has been extended to calculate the fidelity of single-photon teleportation, which allowed us to claim the quantumness of the teleportation process accurately. This demonstration fulfills the requirement for implementation in quantum repeater-based networks.

Finally, by employing SNSPDs with low dead times, an efficient Bell state analyzer was demonstrated for time-bin qubits. The increase of efficiency from 1% to 29% will allow increasing not only the secret key rate for MDIQKD, but also the rates of other protocols involving BSM such as quantum teleportation, entanglement swapping, quantum repeaters etc.

Chapter 7

Outlook

Our current MDIQKD system operates at a clock rate of 20 MHz which results in poor key rates and requires operating the system for long times to extract secret key in finite key regime [3]. Hence, the overall clock rate of the system needs to be improved to a few GHz [62] so that the final key rates achieved are comparable with those of the systems implementing BB84 type QKD protocols. While a MDIQKD network involving three different Alices has been demonstrated already [8], it is necessary to extend this network to a much larger number of users that can be connected on demand to make it more practical. Most of the QKD demonstrations required using dark fibers, which is an expensive and limited resource. Hence, implementations of MDIQKD where the quantum signals are coexisting with strong classical communication signals are highly desired. These three improvements together remove any remaining obstacles for MDIQKD based secure metropolitan networks.

The demonstration of quantum teleportation in a metropolitan fiber network is a significant step towards realizing quantum repeaters. Entanglement swapping using independent sources over a fiber network [117], entanglement swapping into quantum memory compatible photons [118], and entanglement swapping with distant NV centers using 800 nm photons [93] have all been demonstrated. Entanglement swapping into quantum memories where the photons partaking in the BSM are at telecommunication wavelengths and travel over deployed fibers is a highly desired next step. Such a demonstration will pave the way for realizing a practical quantum repeater.

Bibliography

[1] 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] Raju Valivarthi, Qiang Zhou, Caleb John, Francesco Marsili, Varun B Verma, Matthew D Shaw, Sae Woo Nam, Daniel Oblak, and Wolfgang Tittel. A cost-effective measurement-device-independent quantum key distribution system for quantum networks. *Quantum Science and Technology*, 2(4):04LT01, 2017.

[3] Raju Valivarthi, Qiang Zhou, Gabriel H Aguilar, Varun B Verma, Francesco Marsili, Matthew D Shaw, Sae Woo Nam, Daniel Oblak, Wolfgang Tittel, et al. Quantum teleportation across a metropolitan fibre network. *Nature Photonics*, 10(10):676–680, 2016.

[4] J-P Bourgoin, E Meyer-Scott, B L Higgins, B Helou, C Erven, H Hbel, B Kumar, D Hudson, I D'Souza, R Girard, R Laflamme, and T Jennewein. A comprehensive design and performance analysis of low earth orbit satellite quantum communication. *New Journal of Physics*, 15(2):023006, 2013.

[5] Nicolas Gisin, Sylvain Fasel, Barbara Kraus, Hugo Zbinden, and Grégoire Ribordy. Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A*, 73(2):022320, 2006.

[6] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005.

[7] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature photonics*, 4(10):686–689, 2010.

[8] Yan-Lin Tang, Hua-Lei Yin, Qi Zhao, Hui Liu, Xiang-Xiang Sun, Ming-Qi Huang, Wei-Jun Zhang, Si-Jing Chen, Lu Zhang, Li-Xing You, et al. Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Physical Review X*, 6(1):011024, 2016.

[9] Jonathan P. Dowling and Gerard J. Milburn. Quantum technology: the second quantum revolution. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 361(1809):1655–1674, 2003.

[10] Michael A Nielsen and Isaac L Chuang. Quantum computation and quantum information.

[11] Jürgen Brendel, Nicolas Gisin, Wolfgang Tittel, and Hugo Zbinden. Pulsed energy-time entangled twin-photon source for quantum communication. *Physical Review Letters*, 82(12):2594, 1999.

[12] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of modern physics*, 81(2):865, 2009.

[13] Artur K Ekert. Quantum cryptography based on bells theorem. *Physical review letters*, 67(6):661, 1991.

[14] Paul G Kwiat, Klaus Mattle, Harald Weinfurter, Anton Zeilinger, Alexander V Sergienko, and Yanhua Shih. New high-intensity source of polarization-entangled photon pairs. *Physical Review Letters*, 75(24):4337, 1995.

[15] Ivan Marcikic, Hugues De Riedmatten, W Tittel, V Scarani, H Zbinden, and N Gisin. Time-bin entangled qubits for quantum communication created by femtosecond pulses. *Physical Review A*, 66(6):062308, 2002.

[16] Alois Mair, Alipasha Vaziri, Gregor Weihs, and Anton Zeilinger. Entanglement of orbital angular momentum states of photons. *arXiv preprint quant-ph/0104070*, 2001.

[17] Qiang Zhou, Shuai Dong, Wei Zhang, Lixing You, Yuhao He, Weijun Zhang, Yidong Huang, and Jiangde Peng. Frequency-entanglement preparation based on the coherent manipulation of frequency nondegenerate energy-time entangled state. *JOSA B*, 31(8):1801–1806, 2014.

[18] Wolfgang Tittel, Jürgen Brendel, Hugo Zbinden, and Nicolas Gisin. Quantum cryptography using entangled photons in energy-time bell states. *Physical Review Letters*, 84(20):4737, 2000.

[19] Jürgen Volz, Markus Weber, Daniel Schlenk, Wenjamin Rosenfeld, Johannes Vrana, Karen Saucke, Christian Kurtsiefer, and Harald Weinfurter. Observation of entanglement of a single photon with a trapped atom. *Physical Review Letters*, 96(3):030404, 2006.

[20] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical review letters*, 70(13):1895, 1993.

[21] M Żukowski, A Zeilinger, MA Horne, and AK Ekert. event-ready-detectorsbell experiment via entanglement swapping. *Physical Review Letters*, 71(26):4287, 1993.

[22] Klaus Mattle, Harald Weinfurter, Paul G Kwiat, and Anton Zeilinger. Dense coding in experimental quantum communication. *Physical Review Letters*, 76(25):4656,

1996.

[23] Nicolas Sangouard, Christoph Simon, Hugues De Riedmatten, and Nicolas Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Reviews of Modern Physics*, 83(1):33, 2011.

[24] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical review letters*, 108(13):130503, 2012.

[25] Charles Ci Wen Lim, Christopher Portmann, Marco Tomamichel, Renato Renner, and Nicolas Gisin. Device-independent quantum key distribution with local bell test. *Physical Review X*, 3(3):031006, 2013.

[26] E Knill, R Laflamme, and GJ Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409:46–52, 2001.

[27] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen. Bell measurements for teleportation. *Phys. Rev. A*, 59:3295–3300, May 1999.

[28] Warren P Grice. Arbitrarily complete bell-state measurement using only linear optical elements. *Physical Review A*, 84(4):042331, 2011.

[29] Andrea Crespi, Roberta Ramponi, Roberto Osellame, Linda Sansoni, Irene Bongioanni, Fabio Sciarrino, Giuseppe Vallone, and Paolo Mataloni. Integrated photonic quantum gates for polarization qubits. *Nature communications*, 2:566, 2011.

[30] Jeremy L O'Brien, Geoffrey J Pryde, Andrew G White, Timothy C Ralph, and David Branning. Demonstration of an all-optical quantum controlled-not gate. *arXiv preprint quant-ph/0403062*, 2004.

[31] CJ Ballance, TP Harty, NM Linke, MA Sepiol, and DM Lucas. High-fidelity

quantum logic gates using trapped-ion hyperfine qubits. *Physical review letters*, 117(6):060504, 2016.

[32] JH Plantenberg, PC De Groot, CJPM Harmans, and JE Mooij. Demonstration of controlled-not quantum gates on a pair of superconducting quantum bits. *Nature*, 447(7146):836–839, 2007.

[33] D Andrew Golter, Thein Oo, Mayra Amezcua, Kevin A Stewart, and Hailin Wang. Optomechanical quantum control of a nitrogen-vacancy center in diamond. *Physical review letters*, 116(14):143602, 2016.

[34] Tian Zhong, Jonathan M Kindem, Evan Miyazono, and Andrei Faraon. Nanophotonic coherent light-matter interfaces based on rare-earth-doped crystals. *Nature communications*, 6, 2015.

[35] Nicolas Gisin and Rob Thew. Quantum communication. *Nature photonics*, 1(3):165–171, 2007.

[36] S Pirandola, J Eisert, C Weedbrook, A Furusawa, and SL Braunstein. Advances in quantum teleportation. *Nature Photonics*, 9(10):641, 2015.

[37] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[38] Sreraman Muralidharan, Linshu Li, Jungsang Kim, Norbert Lütkenhaus, Mikhail D Lukin, and Liang Jiang. Optimal architectures for long distance quantum communication. *Scientific reports*, 6:20463, 2016.

[39] K. Boone, J.-P. Bourgoin, E. Meyer-Scott, K. Heshami, T. Jennewein, and C. Simon. Entanglement over global distances via quantum repeaters with satellite links. *Phys. Rev. A*, 91:052325, May 2015.

[40] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, et al. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[41] Gary C Kessler. An overview of cryptography.

[42] Claude E Shannon. Communication theory of secrecy systems. *Bell Labs Technical Journal*, 28(4):656–715, 1949.

[43] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[44] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[45] Daniel J. Bernstein and Tanja Lange. Post-quantum cryptography. *Nature*, 549(7671):188–194, 09 2017.

[46] Daniele Micciancio and Oded Regev. Lattice-based cryptography. In *Post-quantum cryptography*, pages 147–191. Springer, 2009.

[47] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.

[48] H Bennett Ch and G Brassard. Quantum cryptography: public key distribution and coin tossing int. In *Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984)*, pages 175–9, 1984.

[49] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of modern physics*, 74(1):145, 2002.

[50] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301, 2009.

[51] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. Secure quantum key distribution. *Nature Photonics*, 8(8):595–604, 2014.

[52] Damien Stucki, Nino Walenta, Fabien Vannel, Robert Thomas Thew, Nicolas Gisin, Hugo Zbinden, S Gray, CR Towery, and S Ten. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New Journal of Physics*, 11(7):075003, 2009.

[53] Alexander R Dixon, ZL Yuan, JF Dynes, AW Sharpe, and AJ Shields. Continuous operation of high bit rate quantum key distribution. *Applied Physics Letters*, 96(16):161102, 2010.

[54] Masahide Sasaki, M Fujiwara, H Ishizuka, W Klaus, K Wakui, M Takeoka, S Miki, T Yamashita, Z Wang, A Tanaka, et al. Field test of quantum key distribution in the tokyo qkd network. *Optics Express*, 19(11):10387–10409, 2011.

[55] Bernd Fröhlich, James F Dynes, Marco Lucamarini, Andrew W Sharpe, Zhiliang Yuan, and Andrew J Shields. A quantum access network. *Nature*, 501(7465):69–72, 2013.

[56] `http://www.idquantique.com;http://www.sequrenet.com;http://www.quintessencelabs.com;http://www.quantum-info.com.`

[57] Jeffrey H Shapiro and Franco N Wong. On-demand single-photon generation using a modular array of parametric downconverters with electro-optic polarization controls. *Optics letters*, 32(18):2698–2700, 2007.

[58] Xiao-song Ma, Stefan Zotter, Johannes Kofler, Thomas Jennewein, and Anton Zeilinger. Experimental generation of single photons via active multiplexing. *Physical Review A*, 83(4):043814, 2011.

[59] Lilian Childress and Ronald Hanson. Diamond nv centers for quantum computing and quantum networks. *MRS bulletin*, 38(2):134–138, 2013.

[60] Julia Benedikter, Hanno Kaupp, Thomas Hümmer, Yuejiang Liang, Alexander Bommer, Christoph Becher, Anke Krueger, Jason M Smith, Theodor W Hänsch, and David Hunger. Cavity-enhanced single-photon source based on the silicon-vacancy center in diamond. *Physical Review Applied*, 7(2):024031, 2017.

[61] Sergio Cova, M Ghioni, A Lacaita, C Samori, and F Zappa. Avalanche photodiodes and quenching circuits for single-photon detection. *Applied optics*, 35(12):1956–1976, 1996.

[62] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W. B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields. Quantum key distribution without detector vulnerabilities using optically seeded lasers. 10:312 EP –, 04 2016.

[63] `https://www.idquantique.com/single-photon-systems/products/id230/`.

[64] Chandra M Natarajan, Michael G Tanner, and Robert H Hadfield. Superconducting nanowire single-photon detectors: physics and applications. *Superconductor science and technology*, 25(6):063001, 2012.

[65] F Marsili, Varun B Verma, Jeffrey A Stern, S Harrington, Adriana E Lita, Thomas Gerrits, Igor Vayshenker, Burm Baek, Matthew D Shaw, Richard P Mirin, et al. Detecting single infrared photons with 93% system efficiency. *Nature Photonics*, 7(3):210–214, 2013.

[66] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C Sanders. Limitations on practical quantum cryptography. *Physical Review Letters*, 85(6):1330, 2000.

[67] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A*, 74(2):022313, 2006.

[68] Antía Lamas-Linares and Christian Kurtsiefer. Breaking a quantum key distribution system through a timing side channel. *Opt. Express*, 15(15):9388–9393, Jul 2007.

[69] Chi-Hang Fred Fung, Bing Qi, Kiyoshi Tamaki, and Hoi-Kwong Lo. Phase-remapping attack in practical quantum-key-distribution systems. *Physical Review A*, 75(3):032314, 2007.

[70] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. Time-shift attack in practical quantum cryptosystems. *Quantum Information & Computation*, 7(1):73–82, 2007.

[71] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A*, 78:042333, Oct 2008.

[72] Nitin Jain, Christoffer Wittmann, Lars Lydersen, Carlos Wiechers, Dominique Elser, Christoph Marquardt, Vadim Makarov, and Gerd Leuchs. Device calibration impacts security of quantum key distribution. *Physical Review Letters*, 107(11):110501, 2011.

[73] Yan-Lin Tang, Hua-Lei Yin, Xiongfeng Ma, Chi-Hang Fred Fung, Yang Liu, Hai-Lin Yong, Teng-Yun Chen, Cheng-Zhi Peng, Zeng-Bing Chen, and Jian-Wei Pan.

Source attack of decoy-state quantum key distribution using phase information. *Physical Review A*, 88(2):022308, 2013.

[74] Audun Nystad Bugge, Sebastien Sauge, Aina Mardhiyah M Ghazali, Johannes Skaar, Lars Lydersen, and Vadim Makarov. Laser damage helps the eavesdropper in quantum cryptography. *Physical review letters*, 112(7):070503, 2014.

[75] Miloslav Dušek, Mika Jahma, and Norbert Lütkenhaus. Unambiguous state discrimination in quantum cryptography with weak coherent states. *Physical Review A*, 62(2):022306, 2000.

[76] Nitin Jain, Birgit Stiller, Imran Khan, Vadim Makarov, Christoph Marquardt, and Gerd Leuchs. Risk analysis of trojan-horse attacks on practical quantum key distribution systems. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):168–177, 2015.

[77] Philippe Grangier, Juan Ariel Levenson, and Jean-Philippe Poizat. Quantum non-demolition measurements in optics. *Nature*, 396(6711):537–542, 1998.

[78] N Sinclair, K Heshami, C Deshmukh, D Oblak, C Simon, and W Tittel. Proposal and proof-of-principle demonstration of non-destructive detection of photonic qubits using a tm: Linbo3 waveguide. *Nature communications*, 7, 2016.

[79] Xiang-Bin Wang. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Physical Review A*, 87(1):012320, 2013.

[80] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91:057901, Aug 2003.

[81] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.*, 94:230503, Jun 2005.

[82] Michael G Tanner, Vadim Makarov, and Robert H Hadfield. Optimised quantum hacking of superconducting nanowire single-photon detectors. *Optics express*, 22(6):6734–6748, 2014.

[83] ZL Yuan, JF Dynes, and AJ Shields. Avoiding the blinding attack in qkd. *Nature Photonics*, 4(12):800–801, 2010.

[84] Charles Ci Wen Lim, Nino Walenta, Matthieu Legré, Nicolas Gisin, and Hugo Zbinden. Random variation of detector efficiency: A countermeasure against detector blinding attacks for quantum key distribution. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):192–196, 2015.

[85] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Physical review letters*, 113(14):140501, 2014.

[86] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

[87] Stefano Pironio, Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009.

[88] Artur Ekert and Renato Renner. The ultimate physical limits of privacy. *Nature*, 507(7493):443–447, 03 2014.

[89] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical review letters*,

23(15):880, 1969.

[90] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2):419, 2014.

[91] John F Clauser and Michael A Horne. Experimental consequences of objective local theories. *Physical review D*, 10(2):526, 1974.

[92] Philippe H Eberhard. Background level and counter efficiencies required for a loophole-free einstein-podolsky-rosen experiment. *Physical Review A*, 47(2):R747, 1993.

[93] Bas Hensen, Hannes Bernien, Anaïs E Dréau, Andreas Reiserer, Norbert Kalb, Machiel S Blok, Just Ruitenberg, Raymond FL Vermeulen, Raymond N Schouten, Carlos Abellán, et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.

[94] Lynden K Shalm, Evan Meyer-Scott, Bradley G Christensen, Peter Bierhorst, Michael A Wayne, Martin J Stevens, Thomas Gerrits, Scott Glancy, Deny R Hamel, Michael S Allman, et al. Strong loophole-free test of local realism. *Physical review letters*, 115(25):250402, 2015.

[95] Marissa Giustina, Marijn AM Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, et al. Significant-loophole-free test of bells theorem with entangled photons. *Physical review letters*, 115(25):250401, 2015.

[96] Wenjamin Rosenfeld, Daniel Burchardt, Robert Garthoff, Kai Redeker, Norbert Ortegel, Markus Rau, and Harald Weinfurter. Event-ready bell test using entangled atoms simultaneously closing detection and locality loopholes. *Physical Review Letters*, 119(1):010402, 2017.

[97] Charles Ci Wen Lim, Christopher Portmann, Marco Tomamichel, Renato Renner, and Nicolas Gisin. Device-independent quantum key distribution with local bell test. *Physical Review X*, 3(3):031006, 2013.

[98] Eli Biham, Bruno Huttner, and Tal Mor. Quantum cryptographic network based on quantum memories. *Physical Review A*, 54(4):2651, 1996.

[99] Hitoshi Inamori. Security of practical time-reversed epr quantum key distribution. *Algorithmica*, 34(4):340–365, 2002.

[100] M Curty, F Xu, W Cui, CC Lim, K Tamaki, and HK Lo. Finite-key analysis for measurement-device-independent quantum key distribution. *Nature communications*, 5:3732–3732, 2014.

[101] Masato Koashi and Andreas Winter. Monogamy of quantum entanglement and other correlations. *Physical Review A*, 69(2):022309, 2004.

[102] Allison Rubenok, Joshua A Slater, Philip Chan, Itzel Lucio-Martinez, and Wolfgang Tittel. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Physical review letters*, 111(13):130501, 2013.

[103] Yang Liu, Teng-Yun Chen, Liu-Jun Wang, Hao Liang, Guo-Liang Shentu, Jian Wang, Ke Cui, Hua-Lei Yin, Nai-Le Liu, Li Li, et al. Experimental measurement-device-independent quantum key distribution. *Physical review letters*, 111(13):130502, 2013.

[104] T Ferreira da Silva, D Vitoreti, GB Xavier, GC do Amaral, GP Temporao, and JP von der Weid. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Physical Review A*, 88(5):052303, 2013.

[105] Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, and Hoi-Kwong Lo. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Physical review letters*, 112(19):190503, 2014.

[106] Yan-Lin Tang, Hua-Lei Yin, Si-Jing Chen, Yang Liu, Wei-Jun Zhang, Xiao Jiang, Lu Zhang, Jian Wang, Li-Xing You, Jian-Yu Guan, et al. Measurement-device-independent quantum key distribution over 200 km. *Physical review letters*, 113(19):190501, 2014.

[107] Yan-Lin Tang, Hua-Lei Yin, Si-Jing Chen, Yang Liu, Wei-Jun Zhang, Xiao Jiang, Lu Zhang, Jian Wang, Li-Xing You, Jian-Yu Guan, et al. Field test of measurement-device-independent quantum key distribution. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):116–122, 2015.

[108] Feihu Xu, He Xu, and Hoi-Kwong Lo. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Physical Review A*, 89(5):052333, 2014.

[109] Yi-Heng Zhou, Zong-Wen Yu, and Xiang-Bin Wang. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Physical Review A*, 93(4):042324, 2016.

[110] Hua-Lei Yin, Teng-Yun Chen, Zong-Wen Yu, Hui Liu, Li-Xing You, Yi-Heng Zhou, Si-Jing Chen, Yingqiu Mao, Ming-Qi Huang, Wei-Jun Zhang, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical review letters*, 117(19):190501, 2016.

[111] Raju Valivarthi, Itzel Lucio-Martinez, Philip Chan, Allison Rubenok, Caleb John, Daniel Korchinski, Cooper Duffin, Francesco Marsili, Varun Verma, Mathew D

Shaw, et al. Measurement-device-independent quantum key distribution: from idea towards application. *Journal of Modern Optics*, 62(14):1141–1150, 2015.

[112] Chao Wang, Zhen-Qiang Yin, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Measurement-device-independent quantum key distribution robust against environmental disturbances. *Optica*, 4(9):1016–1023, Sep 2017.

[113] Chao Wang, Shuang Wang, Zhen-Qiang Yin, Wei Chen, Hong-Wei Li, Chun-Mei Zhang, Yu-Yang Ding, Guang-Can Guo, and Zheng-Fu Han. Experimental measurement-device-independent quantum key distribution with uncharacterized encoding. *Opt. Lett.*, 41(23):5596–5599, Dec 2016.

[114] Feihu Xu, Marcos Curty, Bing Qi, and Hoi-Kwong Lo. Practical aspects of measurement-device-independent quantum key distribution. *New Journal of Physics*, 15(11):113007, 2013.

[115] Chao Wang, Xiao-Tian Song, Zhen-Qiang Yin, Shuang Wang, Wei Chen, Chun-Mei Zhang, Guang-Can Guo, and Zheng-Fu Han. Phase-reference-free experiment of measurement-device-independent quantum key distribution. *Physical review letters*, 115(16):160502, 2015.

[116] Zhen-Qiang Yin, Shuang Wang, Wei Chen, Hong-Wei Li, Guang-Can Guo, and Zheng-Fu Han. Reference-free-independent quantum key distribution immune to detector side channel attacks. *Quantum information processing*, 13(5):1237–1244, 2014.

[117] Qi-Chao Sun, Ya-Li Mao, Yang-Fan Jiang, Qi Zhao, Si-Jing Chen, Wei Zhang, Wei-Jun Zhang, Xiao Jiang, Teng-Yun Chen, Li-Xing You, et al. Entanglement swapping with independent sources over an optical-fiber network. *Physical Review A*, 95(3):032306, 2017.

[118] Jeongwan Jin, M Grimau Puigibert, Lambert Giner, Joshua A Slater, Michael RE Lamont, Varun B Verma, MD Shaw, Francesco Marsili, Sae Woo Nam, Daniel Oblak, et al. Entanglement swapping with quantum-memory-compatible photons. *Physical Review A*, 92(1):012329, 2015.

Appendix A

Paper I

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

Journal of Modern Optics 62.14 (2015): 1141-1150.

Raju Valivarthi[ab], Itzel Lucio-Martinez[ab], Philip Chan[ac], Allison Rubenok[abf], Caleb John[ac], Daniel Korchinski[ab], Cooper Duffin[ab], Francesco Marsili[e], Varun Verma[d], Mathew D. Shaw[e], Jeffrey A. Stern[e], Sae Woo Nam[d], Daniel Oblak[ab], Qiang Zhou[ab], Joshua A. Slater[abg] *&* Wolfgang Tittel[ab].

[a] *Institute for Quantum Science and Technology, University of Calgary, Calgary, AB, T2N 1N4, Canada.*

[b] *Department of Physics and Astronomy, University of Calgary, Calgary, AB, T2N 1N4, Canada.*

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

[d] *National Institute of Standards and Technology, Boulder, CO, 80305, USA.*

[e] *Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, 91109, USA.*

[f] *Present Address: School of Physics, HH Wills Physics Laboratory, University of Bristol,*

Tyndall Avenue, Bristol, BS8 1TL, United Kingdom.

[g]*Present Address: Vienna Center for Quantum Science and Technology (VCQ), Faculty of Physics, University of Vienna, A-1090, Vienna, Austria.*

Abstract

We assess the overall performance of our quantum key distribution (QKD) system implementing the measurement-device-independent (MDI) protocol using components with varying capabilities such as different single photon detectors and qubit preparation hardware. We experimentally show that superconducting nanowire single photon detectors allow QKD over a channel featuring 60 dB loss, and QKD with more than 600 bits of secret key per second (not considering finite key effects) over a 16 dB loss channel. This corresponds to 300 km and 80 km of standard telecommunication fiber, respectively. We also demonstrate that the integration of our QKD system into FPGA-based hardware (instead of state-of-the-art arbitrary waveform generators) does not impact on its performance. Our investigation allows us to acquire an improved understanding of the trade-offs between complexity, cost and system performance, which is required for future customization of MDI-QKD. Given that our system can be operated outside the laboratory over deployed fiber, we conclude that MDI-QKD is a promising approach to information-theoretic secure key distribution.

A.1 Introduction

Quantum key distribution (QKD) [1–4] is the most mature application of quantum information processing – it allows two parties (commonly known as Alice and Bob) to exchange information-theoretic secure cryptographic keys. During the past decade, experimental work has focussed on the development of systems delivering secret keys over deployed fiber at high rates [5–7], over hundreds of kilometres [5], and in trusted-node networks [7, 8]. Furthermore, commercial systems are available for purchase [5].

From a theoretical point of view, the security of QKD is guaranteed by the laws of quantum mechanics. However, in practice, the physical devices employed in QKD systems never perfectly agree with theoretical descriptions. This disparity has led to attacks that compromise the security of real systems [6, 7, 10, 12–15, 18, 20, 40–42]. Most importantly, certain attacks [6, 20] known as 'blinding attacks', exploit vulnerabilities of single-photon detectors (SPDs) to allow an eavesdropper to remotely control all SPDs. In fact, the majority of successful attacks have targeted the SPDs of QKD systems.

Protecting practical QKD systems against these 'side-channel' attacks is a difficult problem, which is currently being investigated by many research groups. Some strategies include developing counter-measures to specific attacks [7, 8] and developing techniques to eliminate specific weaknesses of devices [9]. However with such approaches it is difficult to fully characterize and quantify all possible weaknesses and corresponding attacks, and it may be possible for an eavesdropper to circumvent the countermeasure. Another approach is to develop protocols that are intrinsically secure against side-channel attacks, such as device-independent QKD (DI-QKD) [10, 25], in which no devices have to be trusted and security is guaranteed via a loophole-free Bell-inequality violation. Unfortunately, despite much effort [26, 27], a loophole-free Bell test has yet to be achieved and the implementation of DI-QKD therefore seems unlikely in near future.

More recently, several groups have proposed QKD protocols that are intrinsically secure against the most dangerous side-channel attacks, namely all possible (i.e. known or yet-to-be-proposed) detector side-channel attacks, while requiring proper functioning of other devices [4, 16, 30–32]. The first such protocol, known as measurement-device-independent QKD (MDI-QKD) [4], was inspired by time-reversed entanglement-based QKD [14,15] and, for maximum secret key rate, requires a Bell state measurement (BSM) at a central station (henceforth referred to as Charlie) to create entanglement-like correlations between Alice and Bob. Note that even if an adversary completely controls the measurement device (including the detectors) and, e.g. replaces the entangling measurement by any other measurement, he would not gain any information about the cryptographic key. Hence, as no assumptions about the functioning of the measurement apparatus are required, MDI-QKD is intrinsically immune to all detector side-channel attacks. Thus, MDI-QKD provides enhanced security as compared to traditional QKD.

The MDI-QKD protocol has other important benefits. For instance, it is natural to extend the MDI-QKD scheme to star-type network topologies, in which a large number of users is connected to the same central station, i.e. Charlie, who connects pairs of uses on demand. Such a design is more cost-effective per user than quantum networks comprised of individual point-to-point links [8]. Also, MDI-QKD is a natural stepping stone towards quantum repeaters, which is one approach towards truly long-distance quantum communication [36].

On the other hand, similar to the case of quantum repeater-based communication, MDI-QKD faces the challenge of BSMs with photons created by distant, and independent, photonic qubit sources. Such a measurement requires nearly complete indistinguishability of the photons from each source upon arrival at Charlie's, including polarization, temporal and spectral profiles. The latter is determined largely by local properties of the sources and can thus be easily controlled. However, polarization and arrival-time fluctuate due to time-varying properties of the entire quantum channel between the sources and the central station, as birefringence and refractive index of optical fiber are temperature dependent. Ensuring indistinguishability thus requires feedback systems that counteract external environmental changes. The first demonstration of a BSM with photons from independent and widely separated sources was demonstrated only recently [36] – explicitly for MDI-QKD.

Due to its many advantages, MDI-QKD has received much attention from experimental groups and has been demonstrated in several configurations. The feasibility of MDI-QKD was first demonstrated in [36] using time-bin encoding over up to 80 km of spooled fiber as well as over 18.6 km of deployed fiber across a city centre, and in [21] (using the same type of encoding) over 50 km of spooled fiber and with random modulation of all bases and states, as required for actual key distribution. Subsequent experiments employed polarization qubits in a lab setting with quantum signals frequency-multiplexed with classical signals [22], and with pre-set random state and basis modulation [23]. Most recently, MDI-QKD has been demonstrated over 200 km of spooled optical fiber [24], and in fully-automated fashion and over a real-world link [27].

Our previous experiments have demonstrated the proof-of-principle of MDI-QKD over spooled as well as deployed fiber using a particular configuration for Alice, Bob and Charlie [36] (in these measurements, only the quantum channel changed). Here we assess the impact of using components with varying capabilities – single photon detectors and qubit-preparation hardware – on overall system performance, i.e. secret key rates, and maximum tolerable transmission loss. This allows us to develop a better understanding of the trade-offs between complexity, cost, and system performance, which is required for future customization of QKD systems.

This paper is organized as follows: In section A.2, we describe the MDI-QKD protocol and in section A.3, a detailed description of the realization of our MDI-QKD system is presented. In section A.4, we specify different configurations in which our MDI-QKD system is tested and then discuss results of these tests. We conclude in section A.5.

A.2 The MDI-QKD protocol

Sources of quantum states are at Alice's and Bob's stations. To encode classical bits, they randomly choose a basis and a state among the four BB84 states. In the case of time-bin qubits, these may correspond to the states $|e\rangle$ and $|l\rangle$ (i.e. eigenstates of the Pauli operator σ_Z, forming the so-called Z-basis), or to $|+\rangle \equiv (|e\rangle + |l\rangle)/\sqrt{2}$ and $|-\rangle \equiv (|e\rangle - |l\rangle)/\sqrt{2}$ (i.e. eigenstates of the Pauli operator σ_X, forming the so-called X-basis), where $|e\rangle$ and $|l\rangle$ denote the emission of a photon in an early or late temporal mode, respectively. Furthermore, they associate $|e\rangle$ and $|+\rangle$ with a classical bit value of 0, and $|l\rangle$ and $|-\rangle$ with a classical bit value of 1. The qubits are sent through quantum channels to a third station at which Charlie performs a Bell state measurement (see Figure A.1) that projects their joint state onto one of the four maximally entangled Bell states:

$$\begin{aligned} |\psi^{\pm}_{AB}\rangle &= \frac{1}{\sqrt{2}}(|e_A l_B\rangle \pm |l_A e_B\rangle), \\ |\phi^{\pm}_{AB}\rangle &= \frac{1}{\sqrt{2}}(|e_A e_B\rangle \pm |l_A l_B\rangle). \end{aligned} \tag{A.1}$$

Once a sufficient number of qubits has been transmitted [30], Charlie announces which of his joint measurements resulted in one of the four states of Eq. A.1, as well as the result of the measurement (note that to ensure security, Charlie only needs to be able to project onto one Bell state, but access to more Bell states will increase performance). As a next step, Alice and Bob perform a basis reconciliation procedure known as key sifting. In this step, for each successful projection onto a Bell state, Alice and Bob reveal and compare the bases employed to prepare their respective qubits over an authenticated classical channel and keep only the events in which they used the same basis. Next, depending on the result of the BSM and his preparation basis, Bob must post-process his bit values to ensure identical bit values to Alice. For example, Bob performs a bit flip if the announced measurement resulted in $|\psi^-_{AB}\rangle$, which indicates anti-correlated bits in both the X- as well as the Z-basis. Furthermore, due to unavoidable experimental imperfections such as faulty qubit preparation, channel noise and noisy single photon detectors, as well as possible eavesdropping, it is necessary to go through a key distilling process: After publicly revealing a subset of their prepared bit values, Alice and Bob estimate the error rate for each basis independently, and then perform error correction on the Z-basis bits to remove all discrepancies in their Z-keys (i.e. the key bits associated with preparations in the Z-basis). The error rate for the X-basis is used to bound information that an eavesdropper could have obtained during photon transmission and detection; it is removed by means of privacy amplification. The final secret key rate is given by:

$$S \geq [Q^z[1 - h_2(e^x)] - Q^z f h_2(e^z)] \tag{A.2}$$

in which Q refers to the gain (the probability of a projection onto a Bell state per emitted pair of qubits), e indicates error rates (the ratio of erroneous to total projections a Bell state), h_2 is the binary Shannon entropy and f refers to the efficiency of error correction with respect to Shannon's noisy coding theorem. The superscripts x or z indicate to which basis a particular variable refers.

Due to the need for qubits encoded into individual photons, the above-described implementation is currently difficult to implement. However, by taking advantage of so-called decoy states, it is possible to use phase-randomized weak coherent states (i.e. attenuated laser pulses, which sometimes contain more than one photon) [4, 24, 30, 34], which are straightforward to generate with current technology. This is similar to traditional prepare & measure-type protocols [35, 37, 46]. By randomly modulating the

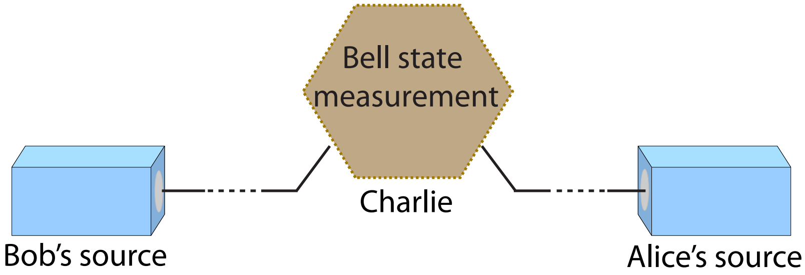


Figure A.1: Schematic of the setup to implement the MDI-QKD protocol. The figure shows two qubit sources labeled as Bob's source and Alice's source that send qubits through a quantum channel to Charlie, a third untrusted party, who performs a Bell state measurement.

mean photon number of the laser pulses between several values known as 'signal' and 'decoy' (the optimal values of which depend on the implementation [38, 39]), one can assess the gains and error rates associated with single-photon emissions. The secret key rate is then given by:

$$S \geq [Q_{11}^{z}[1 - h_2(e_{11}^{x})] - Q_{\mu\sigma}^{z} f h_2(e_{\mu\sigma}^{z})]. \tag{A.3}$$

The '11' subscript indicates values for gain and error rate stemming from Alice and Bob both emitting a single photon, and the subscript '$\mu\sigma$' denotes values associated with mean photon numbers per 'signal' pulse of μ and σ, emitted by Alice's and Bob's, respectively. As in Eq. B.2, the basis is indicated using a superscript.

A.3 Realization of our MDI-QKD system

The experimental setup of our MDI-QKD system can be divided into four parts: qubit preparation, quantum channel, feedback systems, and the BSM unit. We have tested our system with various sources and single photon detectors, and in the following subsections we present a detailed description of each part of our system for each of the configurations used in our MDI-QKD demonstrations.

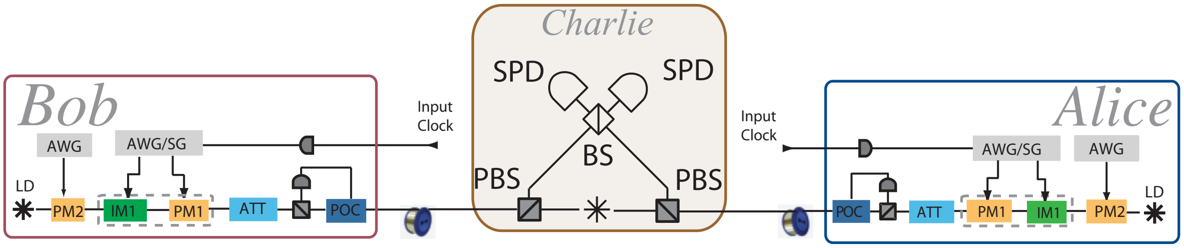


Figure A.2: Experimental setup of our MDI-QKD system (see main text for details). LD: laser diode, PM1 and PM2: phase modulator, IM: intensity modulator, ATT: attenuator, POC: polarization controller and measurement, AWG/SG: arbitrary waveform generator or FPGA-based signal generator (depending on implementation), PBS: polarization beam splitter, BS: beam splitter, SPD: single photon detector.

A.3.1 Qubit preparation

In our MDI-QKD system, Alice and Bob prepare time-bin qubits in one of the four BB84 states introduced above. In our work, time-bin qubits are prepared by externally modulating a continuous wave (CW) laser at 1552 nm wavelength with a commercial intensity modulator (IM1) and a phase modulator (PM1), as depicted in Figure A.2. The time-bin qubits in the X- and Z-basis are prepared by providing different electronic pulses to IM1 and PM1. By changing the attenuation of the optical attenuator (ATT), different mean photon numbers for the time-bin qubits are obtained, as required for the decoy state protocol. In our experiments, the mean photon numbers of the signal and decoy states are optimized through a theoretical model of MDI-QKD to obtain the highest final key rate for each distance [38]. The phase of the qubits is uniformly randomized by applying an electronic signal with randomized amplitudes to PM2, which ensures protection against the unambiguous-state-discrimination (USD) attack [40, 41].

Note that PM2 was not included in some of the measurements described below, and some measurements furthermore employed only one CW laser, whose output was split and sent to Alice and Bob for qubit preparation (deviations from the generic setup depicted in Figure A.2 will be mentioned again in section A.4). It is also worth noting that time-bin qubits can also be prepared using a directly modulated pulsed laser in conjunction with an unbalanced Mach-Zehnder interferometer, IMs and PMs [21].

For our experiments, we use and compare two different electronic driving devices: a commercially-available arbitrary waveform generator (AWG) and a home-made signal generator (SG) based on a field programmable gate array (FPGA) and suitable drivers that transform the FPGA outputs into appropriate analog signals. We developed our signal generator as a cost-effective and compact solution to replace the AWG in anticipation of future development of commercial MDI-QKD system. With the AWG we generate time-bin qubits with a temporal mode width of 100 to 500 ps and a temporal mode separation between 1.5 and 2.5 ns. With our signal generator we generate time-bin qubits with a temporal mode width of 290 ps and a temporal mode separation of 2.5 ns. We characterize the time-bin qubits according to the procedure described in [38]. Motivated by our setups, which create imperfect pure states, we consider time-bin qubits of the form

$$|\psi\rangle = \frac{1}{\sqrt{1+2b^{x,z}}}(\sqrt{m^{x,z}+b^{x,z}}\,|e\rangle + e^{i\phi^{x,z}}\sqrt{1-m^{x,z}+b^{x,z}}\,|l\rangle). \tag{A.4}$$

Here $|e\rangle$ and $|l\rangle$ denote orthogonal early and late temporal modes, respectively. $m^{x,z}$ and $b^{x,z}$ are determined by the properties of the electronic signals from the AWG/SG (e.g. the amplitude, and rising and falling edges of the pulses), and the extinction ratio (ER) of IM1. Furthermore, the superscript indicates to which basis/state the parameter applies (e.g. $m^{z=0}$ applies to the state produces when Alice or Bob chooses the Z-basis state $|l\rangle$). For a perfect time-bin qubit preparation setup, $m^{z=0,1} = 0$ or 1 for qubits in

Table A.1: Measured values for $m^{x,z}$ and $b^{x,z}$ for time-bin qubits prepared using an arbitrary waveform generator (AWG) and our FPGA-based signal generator (SG), respectively.

Parameter	AWG	SG
$b^{z=0,1,x=-,+}$	$(5.34 \pm 0.91) \times 10^{-5}$	$(2.57 \pm 1.18) \times 10^{-5}$
$m^{z=0}$	(0.986 ± 0.012)	(0.982 ± 0.010)
$m^{z=1}$	0	0
$m^{x=-,+}$	(0.4963 ± 0.0042)	(0.4963 ± 0.0062)
$\phi^{z=0,1}= \phi^{x=+}[rad]$	0	0
$\phi^{x=-}[rad]$	$\pi + (0.075 \pm 0.015)$	$\pi + (0.075 \pm 0.015)$

the Z-basis, and $m^{x=+,-} = 0.5$ for qubits in the X-basis; $\phi^{x=+,-} = 0$ or π for qubits in the X-basis (in the Z-basis ϕ^{z} is irrelevant) and $b^{x,z}$ would be zero. We measured these parameters for both implementations; the results are given in Table A.1. As one can see, the parameters barely change when moving from an AWG to our signal generator. The impact on overall system performance will be described in section A.4.2.

A.3.2 Quantum channel

After preparing the time-bin qubits, Alice and Bob send them to Charlie through two different quantum channels (i.e. optical fibers). First, we note that loss during transmission (in conjunction with detector noise) increases the error rate, and this limits the maximum distance for MDI-QKD. Second, ideally, the propagation times of the photons through the fibers should remain constant, and the polarization state of the time-bin qubits should not be affected. Unfortunately, both properties change due to dynamic properties of real-world fiber links. Figure A.3 (a) shows the change of the differential arrival time of attenuated laser pulses from Alice's and Bob's, which we previously reported in [36], over a deployed fiber across the city of Calgary; Figure A.3 (b) depicts the overlap between the polarization states of originally horizontally polarized light from Alice and Bob after propagation to Charlie. It can be seen that both the differential arrival time and the overlap of the polarization states vary over time and are correlated to the outside temperature. As shown in Figure A.3, the differential arrival time varies from -1.6 ns to 0.8 ns in three hours (hours 12–15), during which the temperature increases from -14 °C to -4 °C; and the polarization overlap can vary from 0 (orthogonally polarized pulses) to 1 (identically polarized pulses) in much less than one hour. Hence, to realize a stable MDI-QKD system, we developed active feedback subsystems that control the propagation time and polarization fluctuation, the details of which are given in section A.3.3.

A.3.3 Feedback systems

The main technological challenge to implement MDI-QKD is to perform a BSM with photons from independent sources that travelled through two independent fibers. For this measurement, one requires the two photons to be approximately indistinguishable, i.e, they should have sufficient temporal, polarization, and spectral overlap. To this effect, we implement different feedback mechanisms.

Temporal overlap

Charlie distributes optical clock signals (at 10 MHz) to Alice and Bob via a second optical fiber, which they convert to electrical pulses. This master clock is used to synchronize all relevant devices at Alice's, Bob's and Charlie's. To ensure sufficient temporal overlap, Charlie measures the arrival time of Alice's and Bob's pulses independently every few minutes using a time-to-digital converter (TDC) and SPDs. He then applies an appropriate delay to the distributed clock signal to match the arrival time difference of signals emitted at Alice?s and Bob?s within 30 ps.

Polarization overlap

Charlie sends strong vertically polarized light for 250 ms every 10 seconds through the links to Alice and Bob. Alice and Bob measure its polarization and prepare their qubits orthogonal to that. This ensures that the qubits from Alice and Bob, after travelling through the link, will be identically (horizontally) polarized at Charlie and arrive at the BS. Note that the PBSs in Charlie's system ensure that polarization fluctuations transform into added loss, and not decreased indistinguishability. For additional details see [36].

Spectral overlap

Alice and Bob split some of their laser light that is used to prepare qubits and continuously send it to Charlie via the second optical fiber. Charlie monitors the frequency difference between the two lasers using their beat note signal. Whenever the frequency difference is greater than the threshold of 10 MHz, Charlie communicates the frequency difference to Alice. To maintain sufficient spectral overlap, Alice uses a frequency shifter comprising a phase modulator to which appropriate linear phase chirps are applied using a serrodyne modulation signal.

A.3.4 BSM unit

The BSM unit for time-bin qubits consists of a 50:50 beam splitter followed by two SPDs, as shown in Figure A.2. The two-photon projection measurement occurs by overlapping the two photons on the beam splitter – to erase which-way information – and subsequently detecting the two photons. A projection onto $|\psi^-_{AB}\rangle$ is characterized by a coincidence detection in orthogonal temporal modes in different detectors while a projection onto $|\psi^+_{AB}\rangle$ is characterized by a coincidence detection in orthogonal temporal modes in the same detector. All other coincidence detections (i.e., detections in the same temporal mode) project onto product states. It has been shown that the Bell state measurement efficiency (i.e. the probability that two independent photons are projected onto an entangled state) is limited to 50% when using only linear optics and no auxiliary photons [50]. Note that we only monitor projections onto $|\psi^-_{AB}\rangle$ for the results discussed here, which

Table A.2: Properties of various SPDs we employed.

SPD	id201	id210	SNSPD
Dark count probability[a]	$\sim 10^{-4}$	$\sim 10^{-5}$	$\sim 10^{-7}$
Deadtime	10 μs	10 μs	40 ns
Maximum gate rate	8 MHz	100 MHz	free running
Detector efficiency	∼15%	∼15%	∼50%
Maximum count rate	0.1 MHz	0.1 MHz	2 MHz
Afterpulsing[a]	$\sim 10^{-5}$	$\sim 10^{-5}$	~ 0
Temperature	∼ 223 K	∼ 223 K	∼1 K

reduces the maximum efficiency (assuming lossless detection) to 25%. However, BSM projections onto both $|\psi^-_{AB}\rangle$ and $|\psi^+_{AB}\rangle$ have been demonstrated [31].

The performance of the BSM unit, and in turn an MDI-QKD system, is determined by several detector properties, including the detection efficiency η_{det}, noise, gate rate, recovery time, and detector type. For our measurements, we employ three different types of detectors: two different types of InGaAs-based SPDs from idQuantique (id201 and id210), as well as superconducting nanowire single photon detectors (SNSPDs) [45]. The technical specifications are summarized in Table A.2. While the SNSPDs have far superior properties, they are more cumbersome to use due to more stringent cooling requirements.

A.4 Performance of different MDI-QKD configurations–measurements, results and discussion

We tested our system in 5 different configurations (see Table A.3) and over different quantum channels, which allows us to assess the trade-offs between system performance (in terms of secret key rates or maximum distance), complexity, and cost. The configurations are characterized by different qubit-generation hardware (AWG or SG), the number of lasers employed (1 or 2), the presence of PM2 (used to phase-randomize the laser pulses), and the type of SPDs (id201, id210, SNSPD). Quantum channels are either short fibers with variable loss (implemented using variable attenuators), spooled fiber (without additional attenuator), or deployed fiber.

For each configuration, we created the same combination of quantum states and intensities (i.e. signal or decoy states) at Alice's and Bob's until we gathered enough data, and then changed the states and/or the intensities as required by the decoy state protocol described in [24]. Using Eq. A.4, we then calculated the secret key rates per gate and per second, which are shown in Figures A.4 and A.5, respectively (Figure A.4 additionally shows predicted values using the model described in [38]). In the following sections we will discuss the impact of changing components of our QKD system on its performance.

A.4.1 Quantum channels – real-world versus spooled fibers

Configurations 1 and 2 are identical except for the quantum channel – real-world fiber deployed across the city of Calgary, and spooled fiber inside a temperature-controlled laboratory, respectively (these results have already been presented in [36]). In the absence of significant environmental effects on the deployed channel, the corresponding secret key rates would be identical. However, as described above, the differential arrival time and the polarization overlap vary on time-scales of less than a minute. Hence, without

Table A.3: MDI-QKD system configurations assessed in this work. We list the number of lasers used, the presence of PM2, the hardware employed for qubit generation (AWG or SG), and the single photon detectors (id201, id210 or SNSPD). Quantum channels include short fibers with attenuators (ATT), spooled fiber, and deployed fiber across the city of Calgary.

Configuration	Lasers	PM2	Qubit generation	Detector	Channel	Total channel length	Total channel loss
1	2	no	AWG	id201	Deployed	18.6 km	9 dB
2	2	no	AWG	id201	Spool	20, 40, 60 km	9.1, 13.7, 18.2 dB
3	1	yes	AWG	id210	Spool	60, 100 km	13.7, 20 dB
4	1	yes	AWG	SNSPD	ATT	-	16, 40, 60 dB
5	1	yes	SG	SNSPD	ATT	-	16 dB

properly functioning active stabilization, secret key rates would be significantly reduced. However, as one can see in Figure A.4 we find nearly identical secret key rates, indicating that our feedback systems compensate for the environmental fluctuations as well as time-varying laser frequency differences. Note that our feedback systems have bandwidth limitations (which we have not yet assessed), i.e. will compensate only for sufficiently slow fluctuations. This may affect the maximum distance over which our QKD system can be employed outside the laboratory, even if it still delivers secret key over spooled fiber of the same length inside the lab.

A.4.2 Qubit preparation – AWG versus FPGA-based signal generator

Next, we compare the performance obtained with configuration 4 and 5, which only differ in the hardware used for preparing qubits – AWGs or FPGA-based signal generators (SG). Due to bandwidth differences between the AWG and the SG, the parameters of the prepared time-bin qubits – temporal mode width and temporal mode separation – are insignificantly different (see Table A.4). The measured secret key rates per gate for a 16 dB loss channel are shown in Figure A.4, along with our theoretical prediction. We find very good agreement in case of configuration 5 (SG-based qubit preparation), and reasonable agreement in case of configuration 4 (AWG-based qubit preparation). We attribute the difference mainly to statistical fluctuations (both points overlap within their 2σ uncertainty). Hence, we find that our home-made, cost-effective signal generator produces quantum states of similar quality as the state-of-the-art AWG. This conclusion is also supported by the data in Table A.3.1.

Table A.4: Parameters of prepared time-bin qubits for configurations 4 and 5 (see Table A.3).

Devices	Temporal mode width (FWHM) (ps)	Temporal mode separation (ns)
AWG	250	2.50
FPGA board	290	2.50

A.4.3 Impact of different single photon detectors

Configurations 1-5 differ in the single photon detectors employed for the BSM, the quantum channel (deployed fiber, spooled fiber and variable attenuator), the number of lasers used to create qubits, as well as the hardware employed for the latter. However, given that our feedback system operates reliably (as discussed in section A.3.3), and ignoring the small difference between AWG and SG-based qubit creation (see section A.3.1), we assume in the following that all differences in secret key rates have to be attributed to different SPDs. (Detector performance is characterized in Table A.2.) From the data shown in Figures A.4 and A.5, we find that the secret key rate (in bits per gate) is significantly impacted by the use of different detectors.

As expected, because of their superior detection efficiency and lower noise, the key rate per gate for a specific amount of channel loss (i.e. distance) is higher with SNSPDs compared to id201 and id210 InGaAs SPDs. For the same reason, the maximum distance between Alice and Bob is larger. More precisely, the maximum distance over which MDI-QKD can be performed using id201 detectors is 80 km. Using id210 detectors it increases to 125 km, and for SNSPDs we find 430 km (these estimations assume fiber loss of 0.2 dB/km. Note that fibers with less loss are now available [53], but are probably not yet deployed). At distances below ∼50km, the key rate per gate when using id201 detectors is close to that of using id210 detectors because of similar detection efficiencies (solid and dash-dotted curves in Figure A.4), but employing id210 detectors results in greater distances because of their lower noise (refer to Table A.2).

It is worth noting that, as shown in Figure A.5, when using SNSPDs, the secret key rate (in bits per second – not per gate) over low-loss links is limited by the detectors' maximum count rates, in our case around 2 MHz. To ensure that we do not exceed this rate (in which case the detectors would stop operating), we reduce our qubit generation rate from its maximum of 250 MHz to 20 MHz as the quantum channel loss is reduced from 40 dB to 16 dB. Furthermore, when using InGaAs based detectors, the final key rate is always limited by the deadtime we set to minimize the afterpulsing, $\sim 10\ \mu$s. Figure A.5 shows the secret key rate in bits per second when different detectors are employed (the figure also specifies different qubit generation rates). We find the maximum key rate to be 623 Hz (obtained with SNSPDs over a total channel loss of 16 dB), and that the key rate per second is higher using id210 detectors than with id201 detectors. This is due to the lower noise and higher gate rates (25 MHz compared to 2 MHz) of the id210 detectors (for more details see [54]). Note that finite key effects were not taken into account in calculating secret key rates [30].

A.5 Conclusions and Outlook

In conclusion, we have tested MDI-QKD in various configurations, differing mainly in the type of detectors employed, the need for active feedback systems, and the complexity and cost of the hardware used to create time-bin qubits. We find that time-varying properties of optical fibers do not impact the system performance as they can be compensated using simple active feedback systems, and that the system can be operated using FPGA-based qubit creation hardware. These findings demonstrate that MDI-QKD is already suitable for compact and cost-effective real-world implementations, even though the protocol was proposed only in late 2011. Furthermore, we find that secret key rates benefit from using SNSPDs. The drawback of being more expensive and more complex than InGaAs-based SPDs will be largely offset in star-type quantum networks, where a single BSM (i.e. two SNSPDs) can serve a large number of users. Next development steps of our system concern the integration of true random number generators, testing over real-world links exceeding distances of 100 km and in networks, and interfacing with quantum repeaters [55].

Acknowledgements

We acknowledge technical support by Vladimir Kiselyov, discussions with Erhan Saglamyurek and Neil Sinclair, and thank idQuantique for lending us two id210 single photon detectors. This work was supported through Alberta Innovates Technology Futures, the National Science and Engineering Research Council of Canada (through their Discover Grant and CryptoWorks 21 CREATE programs), the Calgary Urban Alliance, the National Nature Science Foundation of China (No. 61405030), the Oversea Academic Training Fund of the University of Electronic Science and Technology of China, the US Defense Advanced Research Projects Agency InPho Program, and the Killam Trusts. Part of the research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. W.T. is a senior fellow of the Canadian Institute for Advanced Research.

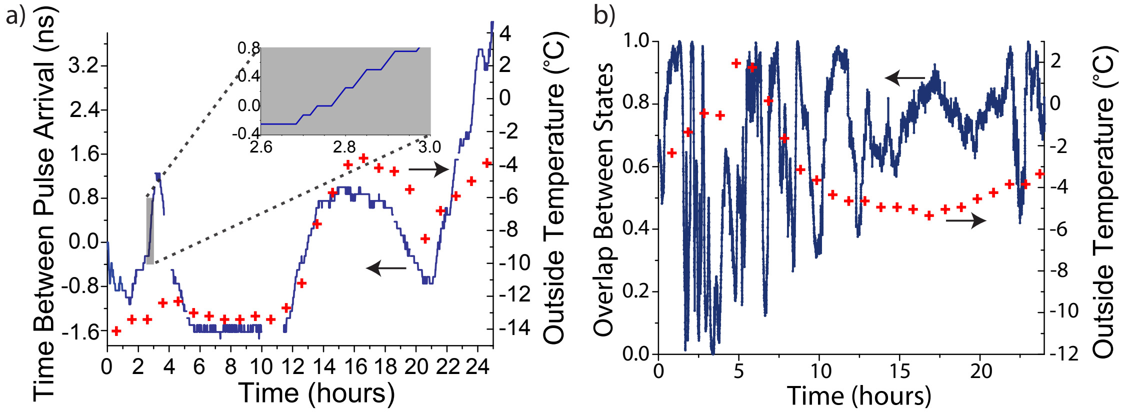


Figure A.3: (a) Differential arrival time of attenuated laser pulses propagation from Alice/Bob to Charlie. (b) Variation in polarization overlap of originally horizontally polarized light propagation from Alice/Bob to Charlie. The temperature data (crosses) is given in the secondary y-axes, showing correlation with variations of differential arrival time and polarization overlap (the figure is identical to that in [36]).

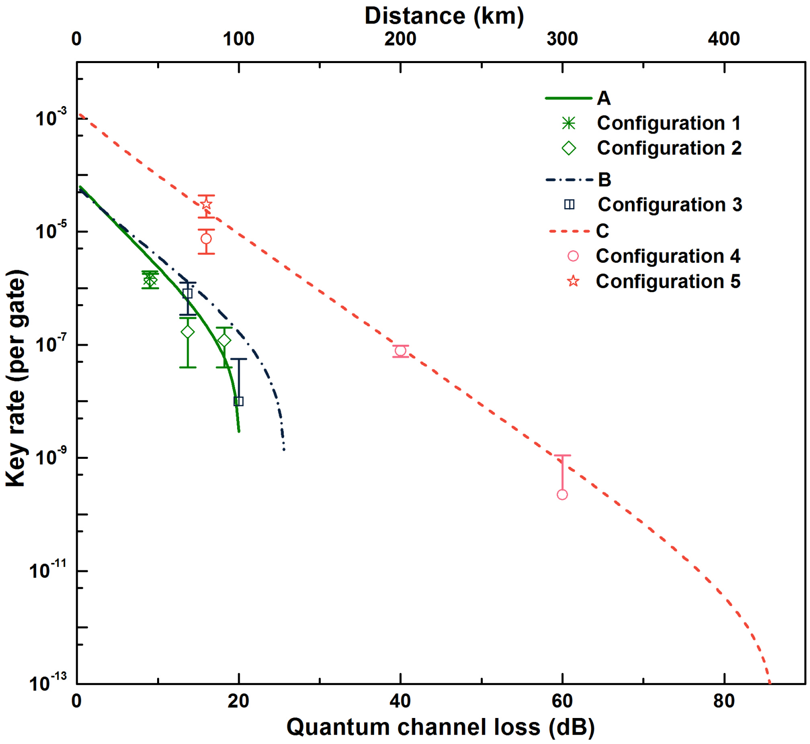


Figure A.4: Experimentally obtained secret key rates per gate versus total loss in the quantum channel. Curve A shows the theoretical prediction assuming configuration 1 or 2, curve B assuming configuration 3, and curve C assuming configuration 4 or 5. Experimentally obtained key rates for the different configurations are plotted as well. All configurations are described in Table A.3. The secondary x-axis shows distance assuming 0.2 dB loss per kilometre of fiber. Uncertainties (one standard deviation) are calculated assuming Poissonian statistics of all measured gains and error rates.

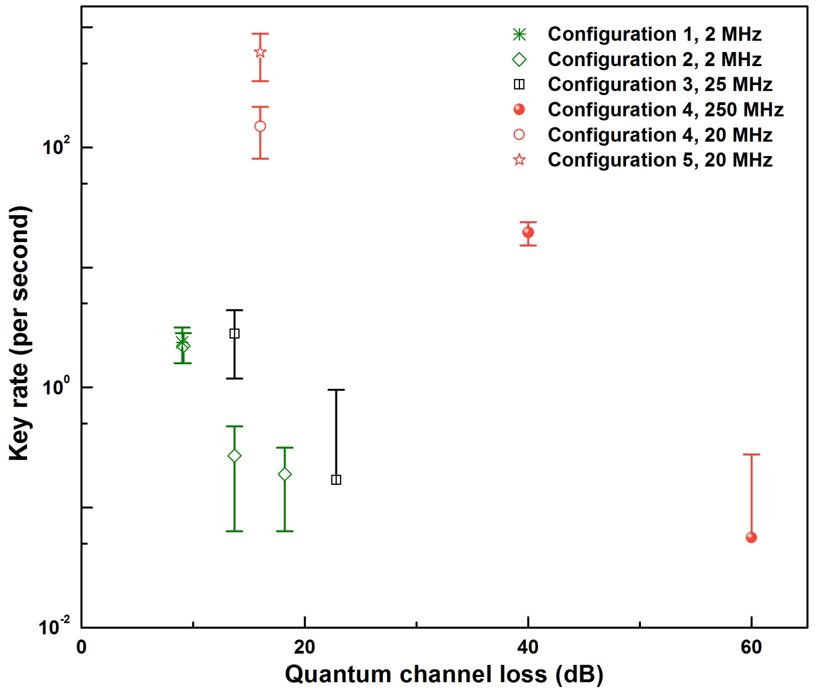


Figure A.5: Secret key rates per second versus loss in the quantum channel for all configurations specified in Table A.3 and for different qubit generation rates. Uncertainties (one standard deviation) are calculated assuming Poissonian statistics of all measured gains and error rates.

Bibliography

[1] C. H. Bennett and G. Brassard, *in Proc. IEEE Int. Conf. Comp. Sys. Sig. Process.* (Bangalore, 1984) pp. 175179.

[2] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, *Rev. Mod. Phys.* **2002**, *74*, 145.

[3] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus and M. Peev, *Rev. Mod. Phys.* **2009**, *81*, 1301.

[4] H.-K. Lo, M. Curty and K. Tamaki, *Nat. Photon.* **2014**, *8*, 595.

[5] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery and S. Ten, *New J. Phys.* **2009**, *11*, 075003.

[6] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe and A. J. Shields, *App. Phys. Lett.* **2010**, *96*, 161102.

[7] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, *Opt. Express* **2011**, *19*, 10387.

[8] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan and A. J. Shields, *Nature* **2013**, *501*, 69.

[9] See http://www.idquantique.com, http://www.sequrenet.com, http://www.quintessencelabs.com, http://www.quantum-info.com.

[10] G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders, *Phys. Rev. Lett.* **2000**, *85*, 1330.

[11] N. Gisin, S. Fasel, B. Kraus, H. Zbinden and G. Ribordy, *Phys. Rev. A* **2006**, *73*, 022320.

[12] V. Makarov, A. Anisimov and J. Skaar, *Phys. Rev. A* **2006**, *74*, 022313.

[13] A. Lamas-Linares and C. Kurtsiefer, *Opt. Express* **2007**, *15* (15), 9388-9393.

[14] C.-H. F. Fung, B. Qi, K. Tamaki and H.-K. Lo, *Phys. Rev. A* **2007**, *75*, 032314.

[15] B. Qi, C.-H. F. Fung, H.-K. Lo and X. Ma, *Quantum Inf. Comput.* **2007**, *7*, 073.

[16] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen and H.-K. Lo, *Phys. Rev. A* **2008**, *78*, 042333.

[17] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, *Nat. Photon.* **2010**, *4*, 686.

[18] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov and G. Leuchs, *Phys. Rev. Lett.* **2011**, *107*, 110501.

[19] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, *Phys. Rev. A* **2013**, *88*, 022308.

[20] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen and V. Makarov, *Phys. Rev. Lett.* **2014**, *112*, 070503.

[21] M. Dušek, M. Jahma and N. Lütkenhaus, *Phys. Rev. A* **2000**, *62* , 022306.

[22] Z. Yuan, J. Dynes and A. Shields, *Nat. Photon.* **2010**, *4*, 800.

[23] C. C. W. Lim, N. Walenta, M. Legré, N. Gisin and H. Zbinden, *arXiv:1408.6398* **2014**.

[24] A. Acìn, N. Brunner, N. Gisin, S. Massar, S. Pironio and V. Scarani, *Phys. Rev. Lett.* **2007**, *98*, 230501.

[25] L. Masanes, S. Pironio and A. Acìn, *Nat. Comm.* **2011**, *2*, 238.

[26] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin and A. Zeilinger, *Nature* **2013**, *497*, 227.

[27] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin and P. G. Kwiat, *Phys. Rev. Lett.* **2013**, *111*, 130406.

[28] H.-K. Lo, M. Curty and B. Qi, *Phys. Rev. Lett.* **2012**, *108*, 130503.

[29] S. L. Braunstein and S. Pirandola, *Phys. Rev. Lett.* **2012**, *108*, 130502.

[30] P. Gonzalez, L. Rebon, T. Ferreira da Silva, M. Figueroa, C. Saavedra, M. Curty, G. Lima, G. B. Xavier and W. A. T. Nogueira, *arXiv:1410.1422* **2014**.

[31] W.-F. Cao, Y.-Z. Zhen, Y.-L. Zheng, Z.-B. Chen, N.-L. Liu, K. Chen and J.-W. Pan, *arXiv:1410.2928* **2014**.

[32] C. C. W. Lim, B. Korzh, A. Martin, F. Bussiéres, R. Thew and H. Zbinden, *arXiv:1410.1850* **2014**.

[33] E. Biham, B. Huttner and T. Mor, *Phys. Rev. A* **1996**, *54*, 2651.

[34] H. Inamori, *Algorithmica* **2002**, *34*, 340.

[35] N. Sangouard, C. Simon, H. de Riedmatten and N. Gisin, *Rev. Mod. Phys.* **2011**, *83*, 33.

[36] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez and W. Tittel, *Phys. Rev. Lett.* **2013**, *111*, 130501.

[37] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang and J. W. Pan, *Phys. Rev. Lett.* **2013**, *111*, 130502.

[38] T. F. da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão and J. P. von der Weid, *Phys. Rev. A* **2013**, *88*, 052303.

[39] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian and H.-K. Lo, *Phys. Rev. Lett.* **2014**, *112*, 190503.

[40] 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, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang and J.-W. Pan, *Phys. Rev. Lett.* **2014**, *113*, 190501.

[41] 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, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang and J.-W. Pan, *IEEE Journal of Selected Topics in Quantum Electronics* **2014**, *21*, 6600407.

[42] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki and H.-K. Lo, *Nat. Comm.* **2014**, *5*, 3732.

[43] X.-B. Wang, *Phys. Rev. A* **2013**, *87*, 012320.

[44] X. Ma, C.-H. F. Fung and M. Razavi, *Phys. Rev. A* **2012**, *86*, 052305.

[45] W.-Y. Hwang *Phys. Rev. Lett.* **2003**, *91*, 057901.

[46] H. K. Lo, X. Ma and K. Chen *Phys. Rev. Lett.* **2005** *94*, 230504.

[47] X.-B. Wang, *Phys. Rev. Lett.* **2005**, *94* , 230503.

[48] F. Xu, H. Xu and H.-K. Lo, *Phys. Rev. A* **2014**, *89*, 052333.

[49] P. Chan, J. A. Slater, I. Lucio-Martinez, A. Rubenok and W. Tittel, *Opt. Express* **2014**, *22*, 12716.

[50] N. Lütkenhaus, J. Calsamiglia and K. A. Suominen, *Phys. Rev. A* **1999**, *59*, 3295.

[51] 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, *Opt. Express* **2014**, *22*, 24497.

[52] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits and S. W. Nam, *Nat. Phot.* **2013**, *7*, 210.

[53] http://www.corning.com

[54] http://www.idquantique.com/photon-counting/support/resource-center-for-infrared-photon-counters.html

[55] N. Sinclair, E. Saglamyurek, H. Mallahzadeh, J. A. Slater, M. George, R. Ricken,M. P. Hedges, D. Oblak, C. Simon, W. Sohler and W. Tittel, *Phys. Rev. Lett.* **2014**, *113*, 053603.

Appendix B

Paper II

A cost-effective measurement-device-independent quantum key distribution system for quantum networks

Quantum Science and Technology, 2 04LT01

Raju Valivarthi[1], Qiang Zhou[1], Caleb John[2], Francesco Marsili[3], Varun B. Verma[4], Matthew D. Shaw[3], Sae Woo Nam[4], Daniel Oblak[1], and Wolfgang Tittel[1]

[1] Department of Physics and Astronomy, and the Institute for Quantum Science and Technology, University of Calgary, Calgary, T2N 1N4, Canada [2] Department of Electrical and Computer Engineering, and the Institute for Quantum Science and Technology, University of Calgary, Calgary, AB, T2N 1N4, Canada [3] Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, 91109, USA [4] National Institute of Standards and Technology, Boulder, CO, 80305, USA

Abstract

We experimentally realize a measurement-device-independent quantum key distribution (MDI-QKD) system. It is based on cost-effective and commercially available hardware such as distributed feedback (DFB) lasers and field-programmable gate arrays (FPGA) that enable time-bin qubit preparation and time-tagging, and active feedback systems that allow for compensation of time-varying properties of photons after transmission

through deployed fibre. We examine the performance of our system, and conclude that its design does not compromise performance. Our demonstration paves the way for MDI-QKD-based quantum networks in star-type topology that extend over more than 100 km distance.

B.1 Introduction

Being the most mature quantum information technology, quantum key distribution (QKD) allows establishing cryptographic keys between two distant users (commonly known as Alice and Bob) based on the laws of quantum mechanics [1–4]. In conjunction with one-time-pad (OTP) encoding, QKD thereby provides a way for provably secure communication, thus promising to end the ongoing battle between codemakers and codebreakers. Many QKD systems, including commercial systems, have been developed during the last 30 years [2–5], and figures-of-merit such as secret key rates and maximum transmission distance continue to improve. However, quantum hacking over the past decade has also established that the specifications of components and devices used in actual QKD systems never perfectly agree with the theoretical description used in security proofs, which can compromise the security of real QKD systems. For instance, the so-called 'blinding attacks' exploit vulnerabilities of single photon detectors (SPDs) to open a side-channel via which an eavesdropper can gain full information about the (assumed-to-be) secure key [6]. Making practical QKD systems secure against all such attacks is a challenging task that has been investigated by many research groups. One approach is to develop attack-specific counter-measures [7–9]. Unfortunately, the success of this strategy strongly depends on how well a QKD system is characterized, and the security of a 'patched' QKD system may be compromised in future due to new and unforeseen attacks. A better solution is to devise and implement protocols that are intrinsically free of all side-channel attacks such as device-independent QKD (DI-QKD) [10], whose security is guaranteed by a loophole-free Bell test. Although such tests have recently been reported [11–13], the implementation of long distance DI-QKD still seems unlikely in the near future.

Several groups, rather than eliminating the vulnerability to all side-channel attacks, have recently started to focus on QKD protocols that are immune to the most dangerous side-channel attacks, i.e. all possible (known or yet-to-be proposed) detector side-channel attacks. One of these protocols is inspired by time-reversed entanglement-based QKD [14–16] and is known as measurement-device-independent QKD (MDI-QKD) [4]. It requires a Bell state measurement (BSM) at a central station, usually referred-to as Charlie, to create entanglement-like correlations between Alice and Bob. The key feature is that even if an eavesdropper completely controls the measurement devices (e.g. by replacing the BSM by another measurement), she would not be able to gain any information about the distributed key without Alice and Bob noticing. This means no assumptions are required about the measurement devices to guarantee the security of MDI-QKD, thus making it intrinsically immune to all detector side-channel attacks. Furthermore, due to the possibility for a large number of users to connect to the same Charlie, point-to-point MDI-QKD is ideally suited for extension into star-type networks. And last but not least, MDI-QKD can be seamlessly upgraded – not disruptively replaced – into quantum repeater-based long-distance quantum communication as more mature hardware becomes available [18, 36].

Due to the above-mentioned advantages, MDI-QKD has received much attention over the past 5 years and has meanwhile been demonstrated by several experimental groups in different configurations. Initial experiments consisted of proof-of-principle demonstrations in a real-world environment with time-bin qubits [20] and in the laboratory using the same encoding but with random selection of bases and states (as is required for secure key generation) [21]. Subsequent demonstrations have included MDI-QKD in the laboratory with polarization qubits [22, 23]. Furthermore, long distance MDI-QKD has been achieved over 200 km and 404 km of spooled optical fiber [24,25], and been mimicked using a short fibre with additional 60 dB loss [26]. More recently, additional point-to-point and network field tests have been implemented [27, 28].

In our previous studies, we have demonstrated a proof-of-principle of MDI-QKD over deployed fibre [20], and also assessed the impact of using different single-photon detectors and different methods for time-bin qubit preparation on the performance of MDI-QKD [26]. The comprehensive understanding of trade-offs among complexity, cost, and system performance acquired through these investigations has now allowed us to develop a complete system, which is described and characterized in the following sections. In particular, our MDI-QKD system now also includes time tagging of qubit generations and detections, which allows key generation from qubits in randomly prepared states, and further improved polarization and arrival-time control of photons travelling from Alice and Bob to Charlie, which ensures their indistinguishability at the moment of the BSM. After examining the overall system performance (i.e. secret key rates and maximally-tolerable transmission loss), we conclude that our cost-effective implementation does not compromise the performance of MDI-QKD. We note that our real-time and continuously-running photon-state control can also be employed in other real-world systems that require stabilization of channels for quantum information transfer, e.g. in quantum teleportation [29].

B.2 Protocol

In the MDI-QKD protocol, the two users – Alice and Bob – prepare qubits randomly in one of the four BB84 states. In the case of time-bin qubits, these are $|e\rangle$, $|l\rangle$, $|+\rangle \equiv$

$(|e\rangle+|l\rangle)/\sqrt{2}$, and $|-\rangle \equiv (|e\rangle-|l\rangle)/\sqrt{2}$. Here, $|e\rangle$ and $|l\rangle$ denote the emission of a photon in an early and late temporal mode, respectively, forming the so-called Z-basis, while $|+\rangle$ and $|-\rangle$ describe superpositions of photon emissions and form the X-basis. Alice and Bob agree that $|+\rangle$ and $|e\rangle$ correspond to a classical bit value of '0', and $|-\rangle$ and $|l\rangle$ to '1'. The prepared qubits are sent to a third party, generally referred-to as Charlie. Charlie performs a BSM that projects the joint state of the two qubits (one from Alice and one from Bob) onto one of the four maximally entangled Bell states,

$$\begin{aligned} |\psi^{\pm}_{AB}\rangle &= \frac{1}{\sqrt{2}}(|e_A l_B\rangle \pm |l_A e_B\rangle), \\ |\phi^{\pm}_{AB}\rangle &= \frac{1}{\sqrt{2}}(|e_A e_B\rangle \pm |l_A l_B\rangle). \end{aligned} \tag{B.1}$$

Once a sufficiently large number of qubits has been transmitted to Charlie [30], he publicly announces which of his joint measurements resulted in one of these four states (photons often get lost during transmission, making a BSM impossible), and he also identifies the measurement result. This allows Alice and Bob to discard the records of qubits that did not generate a successful BSM. It is worth noting that to ensure security, Charlie only needs to be able to project onto one Bell state, but access to more Bell states will increase the key rate in MDI-QKD [31]. Next, based on the information from Charlie, Alice and Bob perform a basis reconciliation procedure known as key sifting. For every successful projection onto a Bell state at Charlie's, Alice and Bob use an authenticated public channel to reveal and compare the preparation bases for their respective qubits, X or Z, and keep only the record of events for which they have picked same basis. Depending on the result of the BSM and the users' preparation bases, Bob must post-process his bit values so that they become identical to Alice's. For instance, Bob performs a bit flip if the announced measurement resulted in $|\psi^{-}_{AB}\rangle$, which indicates anti-correlated bits in both the X- and Z-basis.

Furthermore, due to imperfect qubit preparation, channel noise and noisy single-photon detectors, as well as possible eavesdropping, it is necessary to go through a key distillation process: (1) Alice and Bob publicly reveal a subset of their (non-discarded) bit values, and estimate the error rate for each basis independently; (2) they perform classical error correction on the bits resulting from Z-basis preparation; (3) the error rate for the X-basis is used to bound the information that an eavesdropper could have obtained during photon transmission and detection – it is subsequently removed by means of privacy amplification. This results in a secure key, whose key rate (per clock) is given by:

$$S \geq [Q^Z[1 - h_2(e^X)] - Q^Z f h_2(e^Z)]. \tag{B.2}$$

Here, $Q^{Z(X)}$ refers to the gain, i.e. the probability of a projection onto a Bell state per emitted pair of qubits in either basis; $e^{Z(X)}$ denotes error rates, i.e. the ratio of erroneous to total projections onto a Bell state per emitted pair of qubits prepared in either basis; h_2 is the binary Shannon entropy and $f \geq 1$ characterizes the efficiency of error correction with respect to Shannon's noisy coding theorem.

The above-described protocol, which was originally proposed in 1996 [32], needs qubits encoded into genuine single photons. This is currently difficult to realize due to the lack of high-quality single photon sources. Fortunately, it is possible to overcome this problem by using phase-randomized attenuated laser pulses, which are easy to prepare using commercial technology, in conjunction with the so-called decoy state technique [4, 24, 30, 34–37]. By randomly modulating the mean photon number of the laser pulses between several values known as 'vacuum', 'decoy' and 'signal' [38, 39], one can assess lower and upper bounds on the gain and the error rate associated with Alice's and Bob's laser pulses both containing exactly one photon, respectively. In this case, the secret key rate is given by

$$S \geq [Q_{11}^{Z}[1 - h_2(e_{11}^{X})] - Q_{\mu\sigma}^{Z} f h_2(e_{\mu\sigma}^{Z})]. \tag{B.3}$$

The subscript '11' denotes values for gain and error rate stemming from Alice and Bob both emitting a single photon, and '$\mu\sigma$' denotes values associated with mean photon numbers per emitted pair of 'signal' pulses of μ and σ, respectively. As in Eq. (B.2), the basis is indicated by the superscript.

B.3 Implementation of our MDI-QKD

In this section, we describe the realization of our MDI-QKD system (a schematics is given in Figure B.1). We divide our system into four parts: qubit preparation modules, BSM module, control modules (ensuring indistinguishability of photons arriving at Charlie), and time-tagging module. In the following subsections we describe the implementation of each module.

B.3.1 Qubit preparation modules

As mentioned in section B.2, Alice and Bob need to prepare qubits randomly in one of the four BB84 states. Furthermore, to use attenuated laser pulses as opposed to true single photons as carriers, they also have to vary the pulses' mean photon number and randomize the qubits' global phase. We employ, for both Alice and Bob, a distributed feedback (DFB) laser at 1548 nm wavelength combined with a home-built driver board. By operating the laser below and above the lasing threshold (i.e. operating it in gain-switching mode), we first generate phase-randomized laser pulses whose duration exceed that of the temporal mode (time bin) spacing (we chose pulses of 40 ns duration), which eliminates the possibility of an unambiguous-state-discrimination attack [40, 41]. The pulses are then sent into an intensity modulator (IM) which, depending on the desired

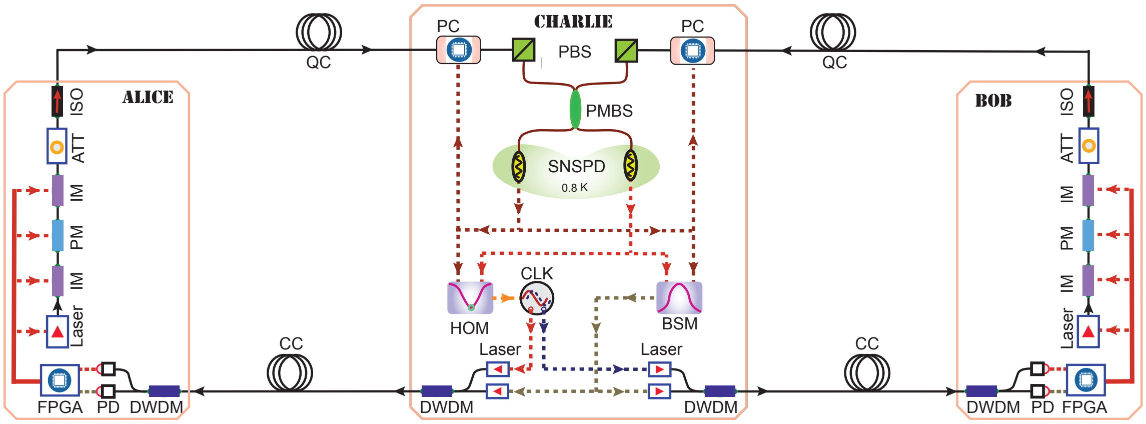


Figure B.1: Experimental setup. PC: polarization controller, PBS: polarization beam splitter, PMBS: polarization maintaining beam splitter, SNSPD: superconducting nanowire single photon detector, HOM: Hong-Ou-Mandel measurement, CLK: clock, BSM: Bell state measurement, DWDM: dense wavelength division multiplexers, PD: photo-detector, FPGA: field-programmable gate array, IM: intensity modulator, PM: phase modulator, ATT: attenuator, ISO: isolator, QC: quantum channel, CC: classical channel. Note that the CLK and BSM signals are distributed to Alice and Bob electronically in the experiment.

qubit state, carves out early and/or late temporal modes of 200 ps duration and with 2.5 ns separation. More precisely Z-basis qubits are generated by carving out an early or a late time bin, while X-basis qubits are generated by carving out an early and a late bin of equal intensity. The electrical pulses applied to the IM are created by an FPGA-based signal generator (SG). We feed the resulting optical signals into a phase modulator (PM) that can apply a phase shift of π to the late mode, as determined by a random binary electronic signal created by the same SG. Hence, the PM only affects qubits in the X-basis for which it generates $|-\rangle$ when the π phase-shift is applied and $|+\rangle$ when it is not. Note, that no distributed phase-reference is required to ensure that X-basis states at Alice and Bob are defined identically. A second IM then allows to rapidly vary the overall intensity of these pulses, and a 99:1 beam-splitter combined with a photodiode (not shown in Fig. B.1) is used in a feedback loop to maximize and maintain the extinction ratio of both IMs combined at about 60 dB. Finally, an optical attenuator allows reducing the intensity of all light pulses to the single photon level, and an optical isolator (ISO) with 50 dB isolation is used to shield Alice and Bob from Trojan horse attacks [42]. The current qubit generation rate is 20 MHz. In our implementation, all electronic signals from the SG board are determined by binary random numbers that have been created off-line using a quantum random number generator (QRNG) [43], and are stored in the FPGA. The QRNG module is in principle compatible with our qubit preparation module, and future work will be aimed at interfacing the two units.

B.3.2 Stabilization and feedback modules

For Charlie to be able to perform a BSM successfully, the photons emitted by Alice and Bob need to be indistinguishable in all degrees of freedom, i.e spatial, spectral, polarization and temporal degrees. The spatial overlap is trivially guaranteed by the use of single mode fibers. The spectral overlap is ensured by carefully tuning and stabilizing the wavelengths of the DFB lasers used for creating qubits. On the other hand, since the photons generally travel long distances (tens of kilometres) through independent fibers, they are subjected to different time-varying environments. This results in fluctuating polarization states and arrival times at Charlie's. It is thus necessary to employ feedback mechanisms to actively compensate for these changes. For efficient key generation, it is desirable for the feedback systems not to interfere with the actual key distribution (ensuring maximum running time for key distribution), and for all the expensive components of the control module to be included into Charlie. This will allow several users in a future star-type network to share these resources, thereby adding to the cost-effectiveness of the network. As described in detail below, the feedback mechanisms used in our implementation satisfy these requirements.

Spectral degree of freedom

To ensure spectral overlap, we employ two continuous-wave DFB lasers with similar bandwidth. We tune their frequency with a resolution of 11.25 MHz by changing the temperatures of the laser diodes until the difference becomes small compared to the spectral width of the created (200 ps long) light pulses, which is 1.26 GHz assuming Gaussian shapes. Towards this end, we interfere unmodulated light emitted by the two lasers into extra fibers on a 50:50 beamsplitter and detect the beat signal (not shown in Fig. B.1). Using a proportional-integral-derivative (PID) feedback loop that acts on the laser temperature, the frequency difference remains below 20 MHz during a period of more than 40 hours. While it is possible to continuously monitor the frequency difference without affecting qubit generation, this was only necessary in the beginning of, but not during, a measurement. In principle the extra fibers can be avoided, e.g. by time-multiplexing the light used to establish the frequency difference (the duty cycle needed for this stabilization would be very small) or by locally using previously agreed-upon and well-defined frequency references.

Polarization degree of freedom

To ensure that the photons coming from Alice and Bob have the same polarization at Charlie, we insert polarization beam splitters (PBSs) at the two inputs of the polarization maintaining beam splitter (PMBS) where the BSM takes place. Polarization fluctuations will thus be mapped onto fluctuations in the count rates of the two superconducting nanowire single photon detectors (SNSPDs) [45] that are used to perform the BSM. These fluctuations control the settings of two polarization controllers (PC, General Photonics, Polastay-POS-002-E) that actively change polarization of input light until the single detector count rates are maximized and hence all polarization changes during photon transmission are compensated for. We emphasize that our method for polarization control does not require extra single photon detectors (SPDs) at Charlie, which differs from the method used in [24]. Moreover our approach results in continuously running polarization feedback, unlike other methods that necessitate interrupting the stream of quantum signals [20, 26].

Timing

Charlie distributes 10 MHz optical signals to Alice and Bob which are converted to electrical signals using a photo detector. This serves as a master clock to synchronize all the relevant devices at Alice, Bob and Charlie. To compensate for varying transmission times from Alice and Bob, respectively, to Charlie, we observe the degree of Hong-Ou-Mandel (HOM) quantum interference at Charlie [29]. To this end, the signals from his two SNSPDs are sent to a HOM unit (in addition to signalling projections onto Bell states, which is further described below), which monitors the rate of coincidence detections corresponding to either both photons arriving in mode $|e\rangle$, or both in mode $|l\rangle$. Thanks to photon bunching, the coincidence count rate reaches a minimum when the photons from Alice and Bob arrive at the PMBS at exactly the same time, providing a precise feedback signal using which we keep arrival times locked. More precisely, we vary Alice's qubit generation time with a precision of 27.8 ps (∼7.2 times less than the width of each temporal mode) to keep the coincidence count rate continuously at the minimum. Thus the arrival times are matched using a free-running feedback mechanism, which does not require the use of additional SNSPDs or high bandwidth PDs [44].

B.3.3 BSM module

The BSM module for time-bin qubit-based MDI-QKD includes a PMBS followed by two SNSPDs, and a fast logical circuit triggered by the electrical signals from the two SNSPDs. For the two-photon projection measurement, the two indistinguishable photons – one from Alice and one from Bob – are overlapped at the PMBS to erase which-way information. A projection onto the $|\psi_{AB}^{-}\rangle$ Bell state is signalled by coincidence detection of two photons (one in each SNSPD) in orthogonal temporal modes (one in $|e\rangle$ and one in $|l\rangle$, while $|\psi_{AB}^{+}\rangle$ corresponds to coincidence detection of two photons in orthogonal temporal modes but in the same detector. It is worth noting that the BSM efficiency is limited to 50% when only linear optics and no auxiliary photons are used [46]. In our implementation, we only select projections onto $|\psi_{AB}^{-}\rangle$ for secret key generation, which reduces the maximum efficiency (assuming lossless detection) to 25%. The coincidence measurement is realized using a home-built broadband logical circuit with a coincidence window of ∼0.7 ns.

B.3.4 Time-tagging module

For any MDI-QKD system, a time-tagging module is needed to record the information of Alice's and Bob's qubit preparations. In our case, this concerns the emission time with a precision of 50 ns plus four bits that specify the basis (X or Z), the bit value (0 or 1), and which out of three different mean photon numbers (vacuum, decoy, signal) have been chosen. Furthermore, the time of a successful BSM at Charlie plus the state projected onto (in our case only $|\psi^-\rangle$) must be registered. Knowing the exact travel times from Alice and Bob, respectively, to Charlie then allows back-tracking and establishing which two qubits have interacted at Charlie. Here we chose a simpler and less memory-intensive approach.

In our MDI-QKD system, Charlie sends a common clock signal to synchronize the qubit preparation devices at Alice and Bob. During the time tagging process, Alice and Bob send the information of their prepared qubits (with the exception of time) into memory buffers, i.e. first-in-first-out (FIFO) buffers in their FPGAs, while the corresponding qubits are sent to Charlie. The memory buffer time is set to be equal to the time required by the qubits to reach Charlie plus the time required by the BSM signals to reach Alice (Bob) from Charlie. A simple logic operation then allows singling out only qubit generations that resulted in a successful BSM – only those are further processed. The clock and BSM signals are sent optically from Charlie to Alice and Bob using another classical channel (CC) with the help of dense wavelength division multiplexers (DWDM) as shown in Fig. B.1. Note that our time-tagging module is integrated in the same FPGA that is also used as a SG (see section B.3.1).

B.4 Experimental results and discussion

We first test the indistinguishability of the photons from Alice and Bob by measuring the visibility of HOM interference using two spooled fibres of 40 km length. Figure B.2 shows the result; the mean photon number is 0.03 per qubit. The circles are the experimentally measured values, while the dashed line is a fit assuming 200 ps wide Gaussian pulses. A visibility of 46.4±0.5% is obtained in our measurement, which is slightly smaller than the

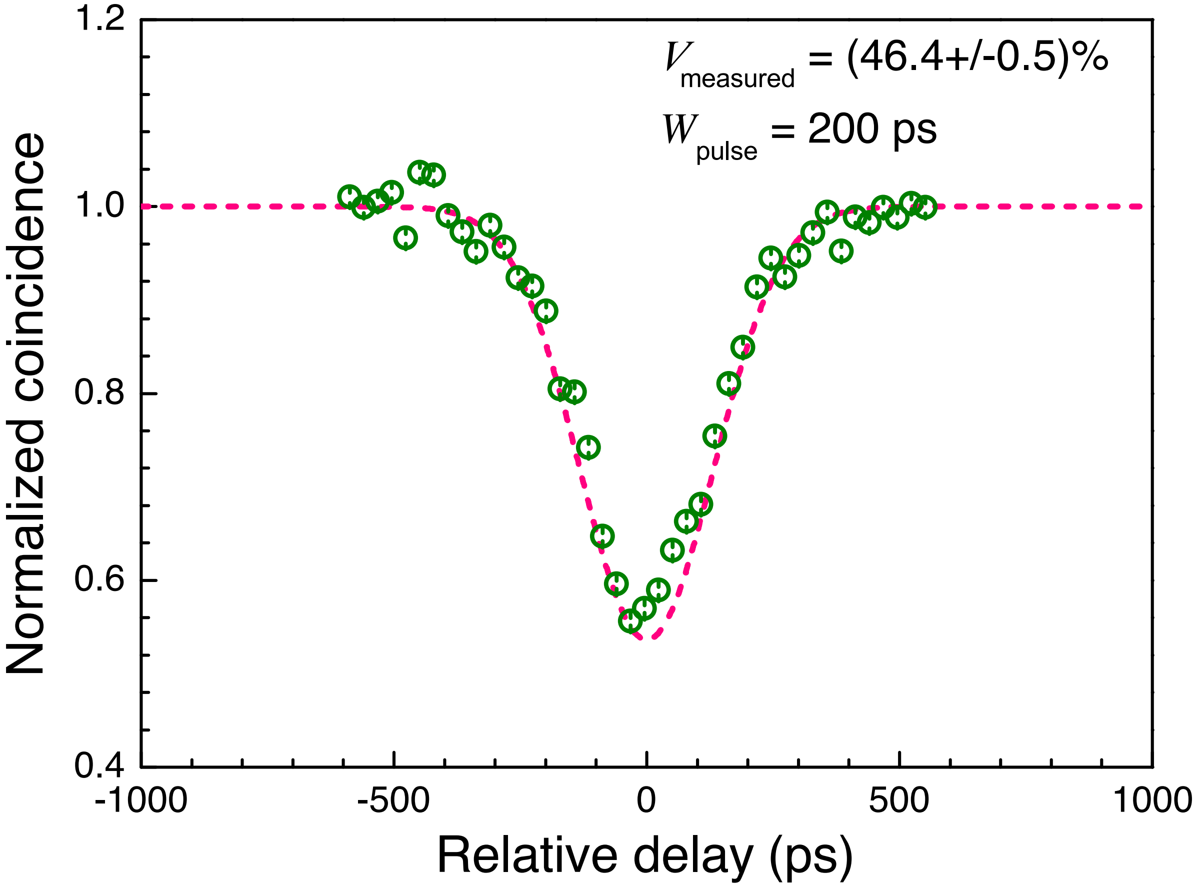


Figure B.2: Result of HOM interference between two independent qubits, encoded into phase-randomized attenuated laser pulses, after each has traveled over 40 km of spooled fiber. Dots show the measured results; the dashed line is the simulation with 200 ps long Gaussian pulses. The maximally achievable visibility is 50%.

maximally possible value of 50% for pulses with Poissonian photon-number distribution. The difference is due to residual distinguishability of the two photons, such as residual difference of spectral and temporal modes and also the finite extinction ratio ($\sim$ 20 dB) of polarizing beam splitters used to filter the polarization before the interference.

Next we run the full QKD system and assess its performance. In the experiment, Alice and Bob prepare time-bin qubits based on pre-stored random numbers and send them to Charlie. Once Charlie successfully projects onto the $|\psi^-\rangle$ Bell state, he sends a signal to Alice and Bob, who tag the corresponding random numbers (i.e. qubit states) on their corresponding time-tagging modules. After sending about 10^{10}, 10^{10}, $10^{10.7}$, and $10^{11.4}$ pairs of qubits over 80, 120, 150 and 200 km of fibre (or over a link with equivalent loss), corresponding in total to the accumulation of about 30 million bytes of tagged data, Alice and Bob compare their files. Based on the gains and quantum bit error rates (QBERs) obtained from this comparison, we calculate the achievable secure key rate [38] in the asymptotic regime, i.e. assuming that our QKD system can run for arbitrarily long time. Figure B.3 shows the experimental results and the theoretical prediction for the different setups used in our demonstrations. The performance is tested with spooled fibre of 2×40 km and 2×60 km (diamonds), and with attenuators simulating lossy quantum channels (circles). We emphasize that all feedback mechanisms are running continuously during the measurements. We find that all measurement results agree well with the prediction (the dashed curve). The gains and QBERs found for 80 km of fiber spool is listed in Table B.1. In particular, the secret key rate over 80 km of spooled fiber is of about 0.1 kbps, which can be improved to around 10 kbps by increasing the clock rate from the current 20 MHz to 2 GHz – the maximum allowed by the 200 ps time-jitter of the SNSPDs [31, 45]. Finally, we note that the performance of our implementation predicts positive secure key rates over up to 400 km assuming (standard) fiber with 0.2 dB loss/km. This distance can be increase to 500 km when using ultra low-loss fibre

(0.16 dB loss/km) as in [25, 47].

The above results are achieved assuming that Alice and Bob are able to send an infinite number of qubits. This is not possible in realistic scenarios and hence statistical fluctuations of finite-size key need to be taken in account to distill the final key. We therefore simulate the performance of our system by extending our theoretical model [38] to include these effects by following the finite-key analysis of MDIQKD from [48] and parameter optimization from [49]. The security parameter for the finite-key analysis is set to $\epsilon = 10^{-7}$. The results of the simulation are shown in Fig. B.4. As can be seen, approximately 10^{11} and 10^{13} pairs of signals have to be sent to get non-zero secure key rates at 100 km and 200 km distances, respectively, which is more than what we did in the above-described demonstrations. With the current repetition rate of 20 MHz, this would take approximately 1.4 and 140 hours of signal exchange. These times can be reduced by a factor of 100 if the repetition rate of the system is increased from 20 MHz to 2 GHz, which is reasonable to achieve in the near future.

B.5 Conclusion and outlook

We have demonstrated a MDI-QKD system based on cost-effective hardware such as commercial DFB lasers; FPGA-based preparation, time-tagging and timing control; and active feedback control for frequency, polarization and arrival-time of photons. Our demonstration paves the way for MDI-QKD-based star-type quantum networks with kbps secret key rates spanning geographical distances in excess of 100 km.

Acknowledgments

We acknowledge technical support by Vladimir Kiselyov. This work was supported through Alberta Innovates Technology Futures, the National Science and Engineering

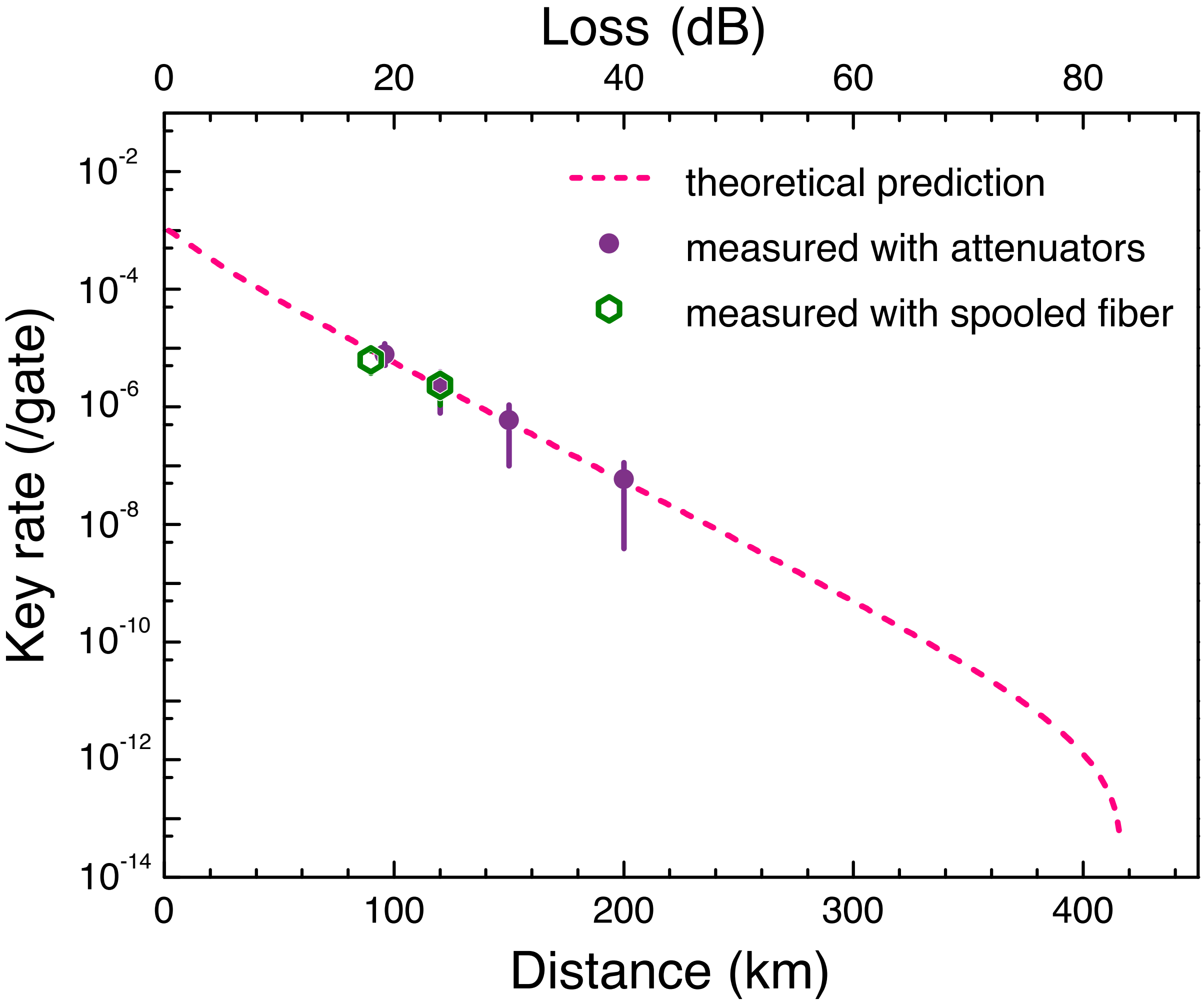


Figure B.3: Secure key rates in the asymptotic regime. Circles denote measured results with attenuators simulating loss in the quantum channels, and diamonds represent measurements with spooled fiber. Uncertainties (one standard deviation) are calculated assuming Poissonian statistics for all measured gains and error rates. Note that finite key effects are not taken into account for the calculation of secret key rates.

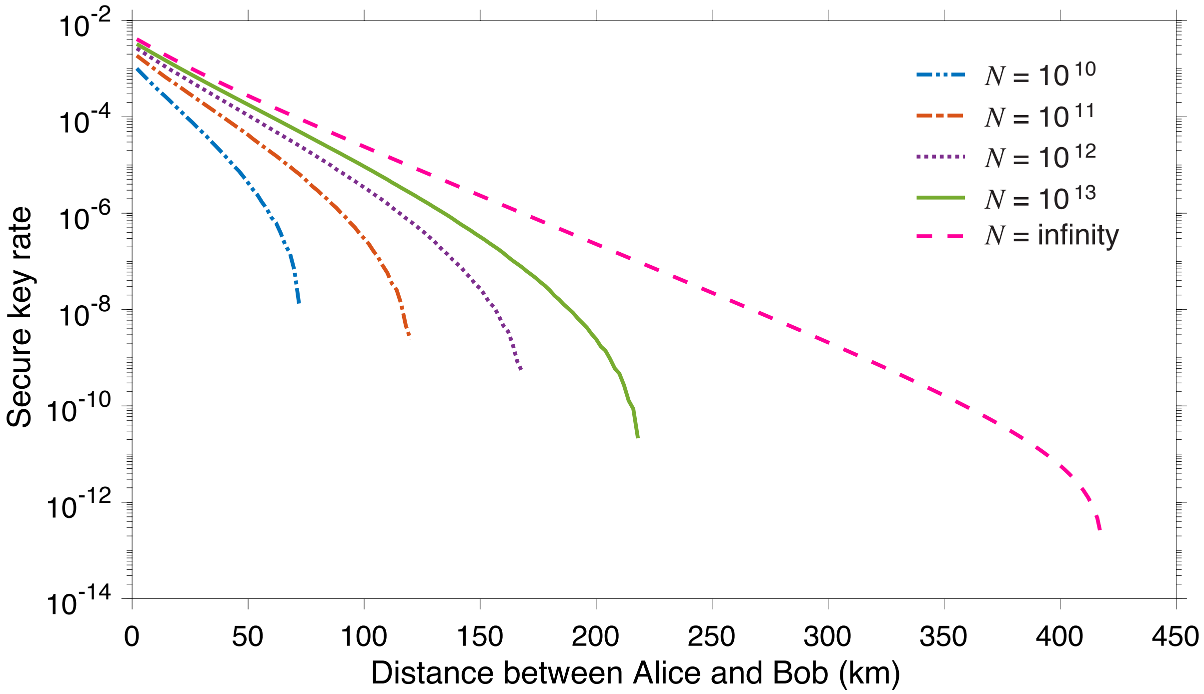


Figure B.4: Simulated secure key rates with and without taking finite-key effects into account. The number N indicates the total number of pairs of qubits emitted by Alice and Bob, and the security parameter is 10^{-7}.

Table B.1: Gains ($Q^{X/Z}_{\mu_A\mu_B}$) and QBERs ($e^{X/Z}_{\mu_A\mu_B}$) for various combinations of signal and decoy states and using 80 km of spooled fibre. Here $\mu_A = \mu_B = 0.53$ and $\nu_A = \nu_B = 0.05$.

	μ_A/μ_B	μ	ν	0
$Q^X_{\mu_A\mu_B}$	μ	5.69×10^{-4}	2.22×10^{-4}	2.03×10^{-4}
	ν	1.63×10^{-4}	9.63×10^{-6}	2.69×10^{-6}
	0	1.56×10^{-4}	2.16×10^{-6}	7.18×10^{-9}
$Q^Z_{\mu_A\mu_B}$	μ	3.44×10^{-4}	3.89×10^{-5}	1.50×10^{-6}
	ν	4.00×10^{-5}	4.48×10^{-6}	2.87×10^{-8}
	0	1.41×10^{-6}	2.87×10^{-8}	1.43×10^{-8}
$e^X_{\mu_A\mu_B}$	μ	0.30	0.41	0.48
	ν	0.41	0.29	0.40
	0	0.47	0.47	0
$e^Z_{\mu_A\mu_B}$	μ	0.01	0.03	0.49
	ν	0.02	0.01	0.38
	0	0.50	0.38	0.25

Research Council of Canada (through their Discovery Grant and the CryptoWorks 21 CREATE programs), and the US Defense Advanced Research Projects Agency InPho Program. Part of the research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. W.T. is a Senior Fellow of the Canadian Institute for Advanced Research.

References

Bibliography

[1] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proc. IEEE Int. Conf. Comp. Sys. Sig. Process* Bangalore, 175–179 (1984).

[2] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden,“Quantum cryptography,” *Rev. Mod. Phys.* **74**(1), 145–195 (2002).

[3] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus and M. Peev, “The security of practical quantum key distribution,” *Rev. Mod. Phys.* **81**(3), 1301–1350 (2009).

[4] H.-K. Lo, M. Curty and K. Tamaki, “Secure quantum key distribution,”*Nat. Photon.* **8**, 595-604 (2014).

[5] www.idquantique.com, www.sequrenet.com, www.quintessencelabs.com, www.quantum-info.com.

[6] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, “Hacking commercial quantum cryptography systems by tailored bright illumination,” *Nat. Photon.* **4**, 686 – 689 (2010).

[7] 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,” *Phys. Rev. A* **78**(4), 042333 (2008).

[8] Z. Yuan, J. Dynes and A. Shields, “Avoiding the blinding attack in QKD,” *Nat. Photon.* **4**, 800–801 (2010).

[9] 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 J. Sel. Top. Quantum Electron.* **21**(2), 1-5 (2015).

[10] A. Acìn, N. Brunner, N. Gisin, S. Massar, S. Pironio and V. Scarani, "Device-Independent Security of Quantum Cryptography against Collective Attacks," *Phys. Rev. Lett.* **98**(23), 230501 (2007).

[11] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abelln, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau and R. Hanson, "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres," *Nature* **526**(7575), 682 – 686 (2015).

[12] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann and A. Zeilinger, "Significant-Loophole-Free test of Bell's Theorem with entangled photons," *Phys. Rev. Lett.* **115**(25), 250401 (2015).

[13] 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, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill and S. W. Nam, "Strong loophole-free test of local realism," *Phys. Rev. Lett.* **115**(25), 250402 (2015).

[14] E. Biham, B. Huttner and T. Mor, "Quantum cryptographic network based on

quantum memories," *Phys. Rev. A* **54**(4), 2651 (1996).

[15] H. Inamori, "Security of practical time-reversed EPR quantum key distribution," *Algorithmica* **34**(4), 340–365 (2002).

[16] S. L. Braunstein and S. Pirandola, "Side-Channel-Free quantum key distribution," *Phys. Rev. Lett.* **108**(13), 130502 (2012).

[17] H.-K. Lo, M. Curty and B. Qi, "Measurement-Device-Independent quantum key distribution," *Phys. Rev. Lett.* **108**(13), 130503 (2012).

[18] A. I. Lvovsky, B. C. Sanders and Wolfgang Tittel, "Optical quantum memory," *Nat. Phot.* **3**, 706–714 (2009).

[19] N. Sangouard, C. Simon, H. de Riedmatten and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Rev. Mod. Phys.* **83**(1), 33 – 80(2011).

[20] 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," *Phys. Rev. Lett.* **111**(13), 130501 (2013).

[21] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang and J. W. Pan, "Experimental Measurement-Device-Independent quantum key distribution," *Phys. Rev. Lett.* **111**(13), 130502 (2013).

[22] T. F. da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão and J. P. von der Weid, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits," *Phys. Rev. A* **88**(5), 052303 (2013).

[23] 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,” *Phys. Rev. Lett.* **112**(19), 190503 (2014).

[24] 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, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang and J.-W. Pan, “Measurement-Device-Independent quantum key distribution over 200 km,” *Phys. Rev. Lett.* **113**(19), 190501 (2014).

[25] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang and J.-W. Pan, “Measurement device independent quantum key distribution over 404 km optical fibre,” *Phys. Rev. Lett.* **117**(19), 190501 (2016).

[26] R. Valivarthi, I. Lucio-Martinez, P. Chan, A. Rubenok, C. John, D. Korchinski, C. Duffin, F. Marsili, V. Verma, M. D. Shaw, J. A. Stern, S. W. Nam, D. Oblak, Q. Zhou, J. A. Slater and W. Tittel, “Measurement-device-independent quantum key distribution: from idea towards application,” *Journal of Modern Optics* **62**(14), 1141-1150 (2015).

[27] 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, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang and J.-W. Pan, “Field test of Measurement-Device-Independent quantum key distribution,” *IEEE Journal of Selected Topics in Quantum Electronics* **21**(3), 6600407 (2015).

[28] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q.

Zhang, T.-Y. Chen and J.-W. Pan, "Measurement-Device-Independent quantum key distribution over untrustful metropolitan network," *Phys. Rev. X* **6**(1), 011024 (2016).

[29] R. Valivarthi, M. G. Puigibert, 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," *Nat. Phot.* **10**, 676–680 (2016).

[30] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki and H.-K. Lo, "Finite-key analysis for measurement-device-independent quantum key distribution," *Nat. Comm.* **5**, 3732 (2014).

[31] 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," *Opt. Express* **22**, 24497 (2014).

[32] E. Biham, T. Mor "Security of Quantum Cryptography against Collective Attacks,"*Phys Rev. Lett.* **78**(11), 2256 (1996).

[33] X.-B. Wang, "Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors,"*Phys. Rev. A* **87**(1), 012320 (2013).

[34] X. Ma, C.-H. F. Fung and M. Razavi, "Statistical fluctuation analysis for measurement-device-independent quantum key distribution," *Phys. Rev. A* **86**(5), 052305 (2012).

[35] W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Phys. Rev. Lett.* **91**(5), 057901(2003).

[36] H. K. Lo, X. Ma and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.* **94**(23), 230504 (2005).

[37] X.-B. Wang, “Beating the Photon-Number-Splitting attack in practical quantum cryptography,” *Phys. Rev. Lett.* **94** (23), 230503 (2005).

[38] P. Chan, J. A. Slater, I. Lucio-Martinez, A. Rubenok and W. Tittel, “Modeling a measurement-device-independent quantum key distribution system,” *Opt. Express* **22**(11), 12716–12736 (2014).

[39] F. Xu, H. Xu and H.-K. Lo, “Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution,” *Phys. Rev. A* **89**(5), 052333 (2014).

[40] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, “Source attack of decoy-state quantum key distribution using phase information,” *Phys. Rev. A* **88** (2), 022308 (2013).

[41] M. Dušek, M. Jahma and N. Lütkenhaus, “Unambiguous state discrimination in quantum cryptography with weak coherent states,” *Phys. Rev. A* **62**(2), 022306 (2000).

[42] N. Gisin, S. Fasel, B. Kraus, H. Zbinden and G. Ribordy, “Trojan-horse attacks on quantum-key-distribution systems,” *Phys. Rev. A* **73**(2), 022320 (2006).

[43] Q. Zhou, R. Valivarthi, C. John and W. Tittel, “Practical quantum random number generator based on sampling vacuum fluctuations,” arXiv:1703.00559 [quant-ph].

[44] Q. Sun, Y. Mao, S. Chen, W. Zhang, Y. Jiang, Y. Zhang, W. Zhang, S. Miki, T. Yamashita, H. Terai, X. Jiang, T. Chen, L. You, X. Chen, Z. Wang, J. Fan, Q. Zhang and J.-W. Pan. “Quantum teleportation with independent sources and prior entanglement distribution over a network,” *Nat. Phot.* **10**, 671–675 (2016).

[45] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits and S. W. Nam, "Detecting single infrared photons with 93% system efficiency," *Nat. Phot.* **7**, 210–214 (2013).

[46] N. Lütkenhaus, J. Calsamiglia and K.-A. Suominen, "Bell measurements for teleportation," *Phys. Rev. A* **59**(5), 3295 (1999).

[47] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nat. Phot.* **9**, 163–168 (2015).

[48] Y. H. Zhou, Z. W. Yu and X. B. Wang, "Making the decoy-state measurement-device-independent quantum key distribution practically useful," *Phys. Rev. A*, **93**(4), 042324 (2016).

[49] F. Xu, H. Xu and H. K. Lo, "Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution," *Phys. Rev. A*, **89**(5), 052333 (2014).

Appendix C

Paper III

Practical quantum random number generation based on sampling vacuum fluctuations

Under review.

Raju Valivarthi[1], Qiang Zhou[1], Caleb John[2] and Wolfgang Tittel[1]

[1] Department of Physics and Astronomy, and the Institute for Quantum Science and Technology, University of Calgary, Calgary, T2N 1N4, Canada [2] Department of Electrical and Computer Engineering, and the Institute for Quantum Science and Technology, University of Calgary, Calgary, AB, T2N 1N4, Canada

Abstract

Quantum random number generation is an enabling technology for applications of quantum information science. For instance, a secure quantum key distribution (QKD) system requires a practical, easily integratable, high-quality and fast random number generator. Here, we propose and demonstrate an approach to random number generation that promises to satisfy these requirements. In our scheme, vacuum fluctuations of the electromagnetic-field inside a laser cavity are sampled in a discrete manner in time and amplified by injecting current pulses into the laser. This results in the generation of laser pulses with random phases. Random numbers can be obtained by interfering the laser pulses with another independent laser operating at the same frequency. Using only

off-the-shelf opto-electronic and fiber-optic components at 1.5 μm wavelength, we demonstrate experimentally the generation of high-quality random bits at a rate of up to 1.5 GHz. With the help of better opto-electronic devices, the generation rate of our scheme can be improved up to tens of GHz. Our results show the potential of the new scheme for practical quantum information applications.

C.1 Introduction

The generation of true random numbers is highly desirable for digital information systems [1–3]. For instance, in quantum key distribution (QKD), random bits are used as a seed for creating secure keys shared between two legitimate users [4–6]. Devices generating random numbers by exploiting the unpredictable nature of quantum processes are known as quantum random number generators (QRNGs) [7–9]. Among all quantum physical systems, photons are possibly the most promising medium as they are easy to generate, manipulate and detect. Taking advantage of current photonics technology, QRNGs have been demonstrated based on the detection of single photon in different modes [10–18], quantum non-locality of entangled pairs of photons [19, 20], phase noise of lasers [21–24], vacuum-seeded bistable processes [27,28], vacuum states [25,26], and vacuum fluctuations in laser cavities [29–33]. Yet, despite intense efforts to develop high-quality and high-speed QRNGs, more work is required for creating simple, cost-effective and practical devices.

In this Letter, we propose and experimentally demonstrate a quantum random number generation scheme that is based on the creation of short laser pulses with quantum-random phases [34]. QRNGs based on such phase randomness have been demonstrated before: by interfering subsequent pulses in an unbalanced Mach-Zender interferometer (UMZI), the phase randomness was mapped onto easily-detectable intensity variations [30–33]. However, due to pulse emission-time jitter, the interference quality degrades significantly as the pulse length approaches the emission-time uncertainty, which limits the minimum pulse width and hence the maximum pulse rate [31, 33]. In our scheme, the phase randomness of laser pulses is converted into intensity fluctuations by interfering them with another (quasi)-continuous wave laser featuring identical central frequency and polarization. The restriction of data acquisition to short time windows aligned – possibly after pulse detection – with the centres of the laser pulses effectively broadens and equalizes the spectra of the continuous wave laser and the pulsed laser, thereby ensuring high interference contrast even at high pulse repetition rates. Thus, our method not only inherently guarantees the temporal overlap needed for good interference, but can also create random numbers with narrower laser pulses and hence higher generation rates. Using only off-the-shelf opto-electronic and fiber-optic components at 1.5 μm wavelength, we perform a proof-of-principle experiment of the proposed scheme and extract high-quality quantum random numbers at a rate of 1.5 GHz. Moreover, we discuss ways to improve the performance, i.e. the generation rate, of our scheme.

C.2 Proposed scheme

Figure C.1 (a) shows the idealized schematic of our random number generation. A semiconductor laser, $L1$, is operated in gain-switched mode. It is first biased far below threshold, i.e. around 0 mA, and then driven significantly above threshold using a short current pulse. This pulse samples and amplifies the vacuum fluctuation of the electromagnetic-field in the laser cavity, which results in the generation of laser pulses with quantum-random phases. Pulses from $L1$ are then superposed with the output of a (quasi)-continuous wave laser, $L2$, using a 50/50 beam splitter (BS). Note that an optical isolator (ISO) is used to avoid all light injecting into $L1$, thereby preventing the generation of phase correlations between laser pulses [35, 36].

The interfering pulses are detected by a balanced photo detector (B-PD). Ignoring detector noise, the differential voltage $\Delta V(t)$ output by the B-PD is

$$\Delta V(t) = 4 \times \eta_d E_1(t) E_2(t) \sin[\varphi_1(t) - \varphi_2(t)], \tag{C.1}$$

where η_d is the efficiency of the B-PD; $E_1(t)$, $E_2(t)$, $\varphi_1(t)$ and $\varphi_2(t)$ are the amplitudes and phases of the light fields from $L1$ and $L2$, respectively; and $t = mT$, where m is an integer and T is the pulse period of $L1$. Since $\varphi_1(t)$ is random, electrical pulses of random amplitudes are obtained from B-PD.

To convert the pulses into raw bits, each pulse is input into an analog-to-digital converter (ADC) that divides the range of possible amplitudes into 2^n bins. (As we explain later, the maximum effective number of bins, $2^{n_{max}}$, that can be achieved is determined by the min-entropy of the signal from the B-PD [30].) The output of the ADC, specified by n bits $b_1, b_2, ..., b_n$, is then sent into a field programmable gate array (FPGA) that performs a randomness extraction procedure, resulting in true quantum-random bits. This procedure requires n randomness extractors (RNEs). Each RNE receives one specific bit $b_i(t)$ per ADC output (see Fig. C.1 (a)). The RNE buffers $2m$ bits during $2m$ periods, then divides them into two m-bit strings, for example $b_i(T), ..., b_i(mT)$ and $b_i(mT + T), ..., b_i(2mT)$. The two m-bit strings are then input into an XOR gate, where elements are XORed element wise, for e.g, $b_i(T)$ with $b_i(mT+T)$, $b_i(2T)$ with $b_i(mT+2T)$ and so on. This creates m bits at the output, as shown in the inset of Fig. C.1 (a). The value of m determines the separation between the two bits that are combined in the XOR gate. A larger m means less correlation between bits. Hence, with a proper value of m, the method presented here is equivalent to using two independent raw-bit sources, as demonstrated in Ref. [27]. We remark that given our randomness extraction procedure is not proven to be information-theoretic secure, the quality of the randomness of the extracted bits is tested using the standard NIST test suite as shown in section C.4 and measuring the auto-correlation of the bits before and after extraction, shown in Fig C.3. Finally, after parallel-to-serial conversion, the bits from all RNEs form a string of ready-to-use random bits. Thus we can achieve an average generation rate of random numbers of $nR/2$, where $R = 1/T$ is the repetition rate of the pulsed laser $L1$. We note that, compared with randomness extraction using a cryptographic hash function [37], the employed RNE method in our scheme imposes less performance on the FPGA and is much easier to implement in real time. However, it may result in losing more random bits than necessary to obtain a final quantum-random bit string.

C.3 Proof-of-principle demonstration

Figure 1 (b) shows a picture of the laser drivers and lasers $L1$ and $L2$ used in our experimental demonstration of the proposed scheme. The central wavelengths of both lasers are at 1540 nm – they are matched and stabilized by controlling the lasers' temperatures within 0.01 degree C. The gain-switched laser is driven by a sequence of current pulses, which are generated from a radio-frequency transistor switched on/off by an FPGA signal. The width of the current pulse is $\sim$200 ps, and the repetition rate is 250 MHz. After interference with the output from the (quasi)-continuous wave laser $L2$ in a polarization maintaining 50/50 BS (used to match the polarization mode, thus maximize the visibility), the optical signals are detected by a commercial B-PD (Thorlabs, PDB480C). It is worth noting that the balanced detection scheme removes all common-mode noise, which results in the improvement of the signal-to-noise ratio of the detection signal. Figure C.1 (c) shows typical signals from B-PD, i.e. $\Delta V(t)$ given in Eq. (C.1). The dashed line is the average of the detected signal.

Please note that, in our proof-of-principle demonstration, the ADC, RNEs and parallel-to-serial conversion described above have not been implemented using an FPGA. Instead, we used a computer to process analog signals from B-PD that have previously been sampled by a fast oscilloscope (Lecroy, 8600A). Hence, while we demonstrate a proof-of-principle of the proposed scheme, the random numbers are not yet generated in real time.

C.4 Results

As shown in Eq. (C.1), the phase uncertainty of the emitted laser pulses affects $\Delta V(t)$ through the interference and balanced photo-detection. Figure C.2 shows the probability density function (PDF) of the normalized $\Delta V(t)$, sampled at pulse center t = mT. The dots represent the experimental results. The solid red line is the theoretical prediction of the corresponding PDF, i.e. $p(x) = 1/(\pi\sqrt{1-x^2})$, where x is the normalized analog output of the B-PD at t=mT, and the phase distribution is assumed to be uniform. We attribute the deviation of our experimental results from the theoretical prediction to additional amplitude fluctuations in the detection signal that stem from classical sources, such as peak power fluctuations of laser pulses, limited bandwidth of the B-PD, finite sampling rate, and noise of the oscilloscope. We estimate the extent of these amplitude fluctuations by inputting the laser pulses from $L1$ into one of the photo-detectors of the B-PD and analyzing its output using the same oscilloscope. Ideally, without the above-mentioned fluctuations, we would expect a constant output from that detector. However, we found an electrical signal whose amplitude follows a Gaussian distribution with standard deviation of $\leq 5\%$ compared to the full range of the observed electrical signal. We simulate the effect of these classical fluctuations by adding them to the predicted values for the ideal case using a Monte-Carlo method. The dashed line in

Fig. C.2 shows the good agreement of the result with the measured data. This allows us not only to verify that the phase of each pulse is indeed random (but not fully quantum-random), but also suggests ways to improve the quality of the random numbers, such as using a B-PD and ADC with large bandwidth.

One of the main advantages of this random number generation scheme is that more than one random bit can be obtained per detection. The total range of the measured signal can be divided into 2^n bins, and each signal represented by n bits. The maximum number of bits, n_{max}, that can be extracted is determined by the min-entropy of the analog signal from B-PD,

$$H_{min} = -log_2(p_{max}) \tag{C.2}$$

where p_{max} is the maximum probability for the detection amplitude to belong into any of the 2^n bins. By increasing the number of bins, we find that H_{min} saturates at 12.8 for $n \geq 13$, indicating that $n_{max} = 12$ raw random bits can be extracted from each pulse [30]. To improve the quality of randomness, we employ the randomness extraction procedure described in section C.2, which reduces the information per laser pulse from 12 to 6 bits. Therefore, with a clock rate of 250 MHz, 12-bit binning and the randomness extraction, random bits are obtained at 1.5 GHz rate, which is half of the maximum of 3.0 GHz = 12 × 250 MHz.

To show the quality of the final random bits obtained from our setup, we first create a 1 Gbit-long random file by saving measurement results from the oscilloscope and processing them in the computer. We measure auto-correlation of the processed random bits before and after randomness extraction and the results are shown in Fig. C.3. We also subject the random bits to the NIST statistical suite, which is a battery of fifteen tests used to analyze the statistical properties of random numbers [38]. By monitoring the results of the NIST test as a function of m (i.e. the length of the buffer in the RNEs), we find that with $m = 7$, the obtained random file passes all the tests.

For the NIST test, the significance level (α) is set at 0.01 as suggested by the test suite [38], implying that one out of one hundred tests is expected to fail even if the random numbers being tested are generated by a fair random generator. Each of the fifteen tests is considered to be a success if the proportion of success versus fail is within a range given by $\hat{p} \pm 3\sqrt{\hat{p}(1-\hat{p})/N}$, where N is the number of times an individual test runs (i.e. $N=$ 1000 in our case), and $\hat{p} = 1-\alpha$. This results in the proportion value greater than 0.9806 and less than 0.9994 in our case, which is the range of green-dashed bar as shown in Fig. C.4 (a). Next, a P-value is obtained for each test from the distribution of P-values over 1000 trials. It is considered a pass if this P-value is above the suggested significance level of 0.0001 [32]. As shown in Fig. C.4, our data passes all the NIST tests.

C.5 Conclusion

We introduced and reported a proof-of-principle demonstration of a new scheme for creating high quality quantum-random bits based on a gain-switched and a (quasi)-continuous wave laser. The generation rate, currently 1.5 Gbps, can be further increased by operating the gain-switched laser with higher repetition rate. While this rate is fundamentally limited due to the need for laser cavity depletion in-between subsequent pulses, rates of several GHz for gain-switched laser are feasible [32, 33]. Combined with the possibility to create more than 10 random bits per laser pulse, we therefore predict that our scheme can deliver high-quality quantum random numbers at rates of many tens of GHz.

We note that, while the present work was being finalized, a related experimental demonstration using a photonics chip has been reported [39, 40].

Funding Information

This work was funded through Alberta Innovates Technology Futures (AITF), and the National Science and Engineering Research Council of Canada (NSERC). WT furthermore acknowledges funding as a Senior Fellow of the Canadian Institute for Advanced Research (CIFAR).

Acknowledgments

The authors thank Vladimir Kiselyov for technical support, and Daniel Oblak and Carlos Abellán for useful discussions.

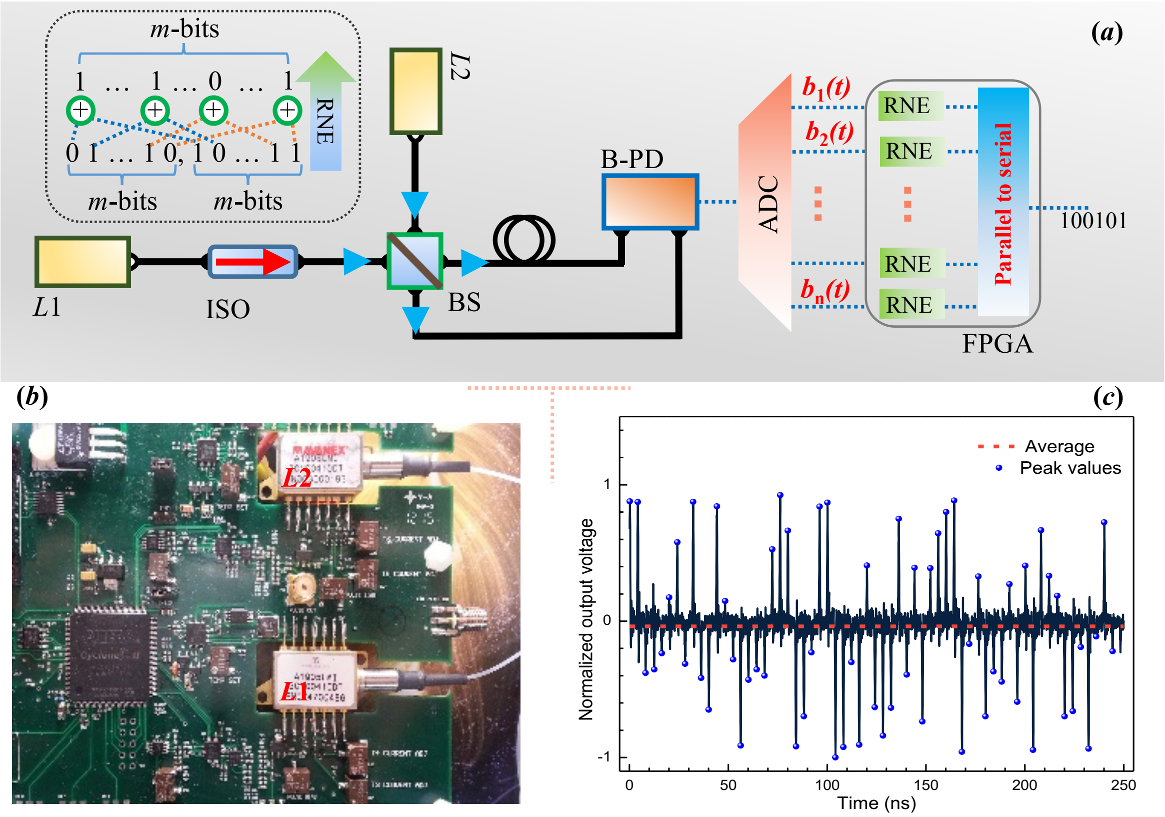


Figure C.1: (a) Schematic of our random number generator; (b) Picture of PCB board with gain-switched (pulsed) laser and (quasi)-continuous wave laser; (c) Typical signal from balanced-photo detector. $L1$: gain-switched laser; $L2$: (quasi)-continuous wave laser; ISO: optical isolator; BS: 50/50 beam splitter; B-PD: balanced-photo detector; ADC: analog to digital converter; RNE: randomness extractor; XOR: exclusive OR gate; VEDL: variable electronic delay line; SW: switch; CLK: clock; FPGA: field programmable gate array.

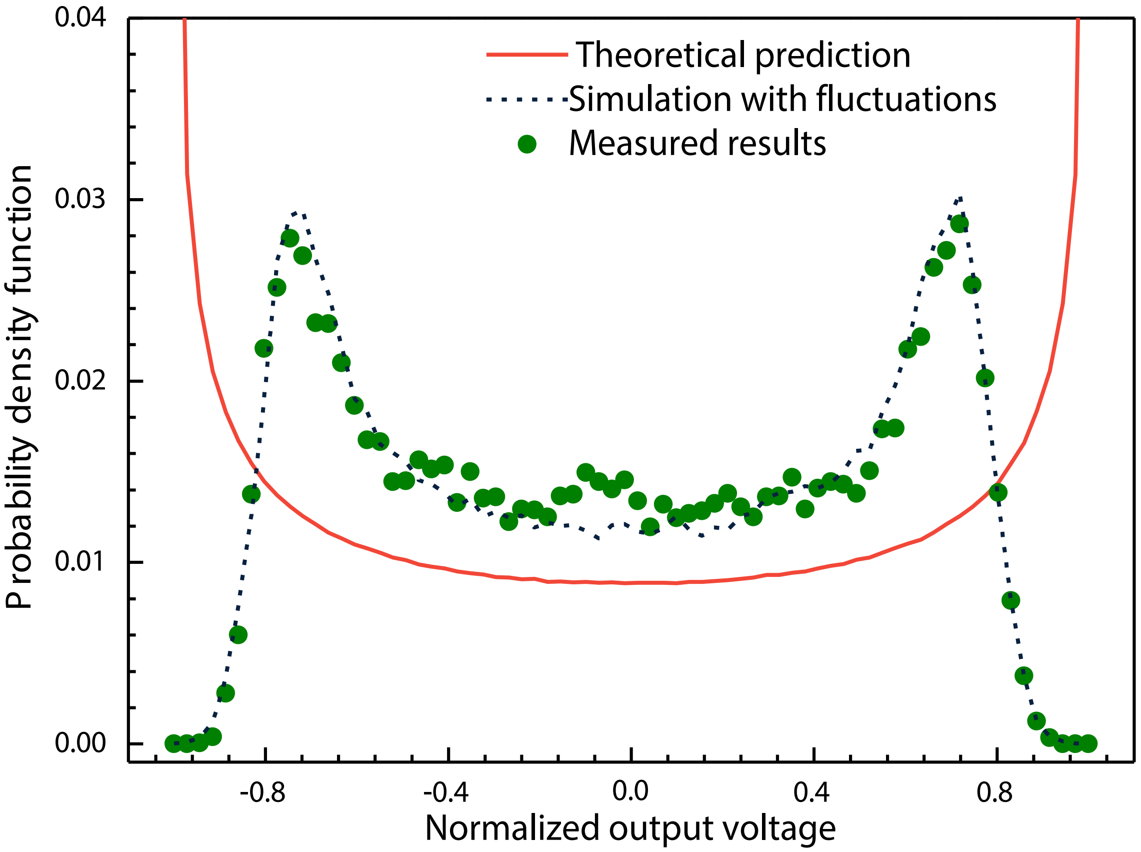


Figure C.2: Probability density function of the normalized analog signals, $\Delta V(t)$

.

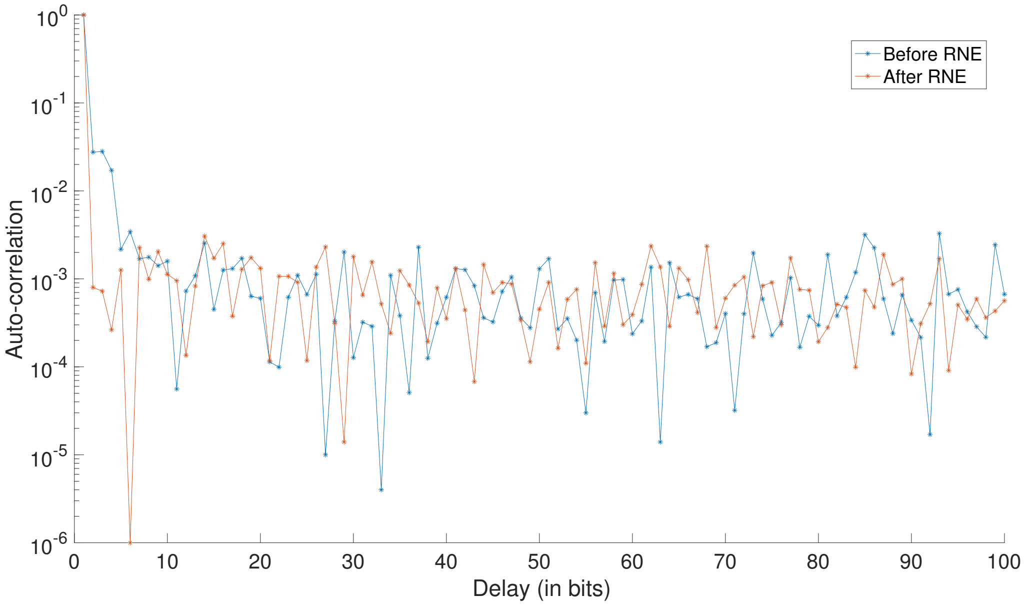


Figure C.3: Auto-correlation results for the random bits before and after extraction.

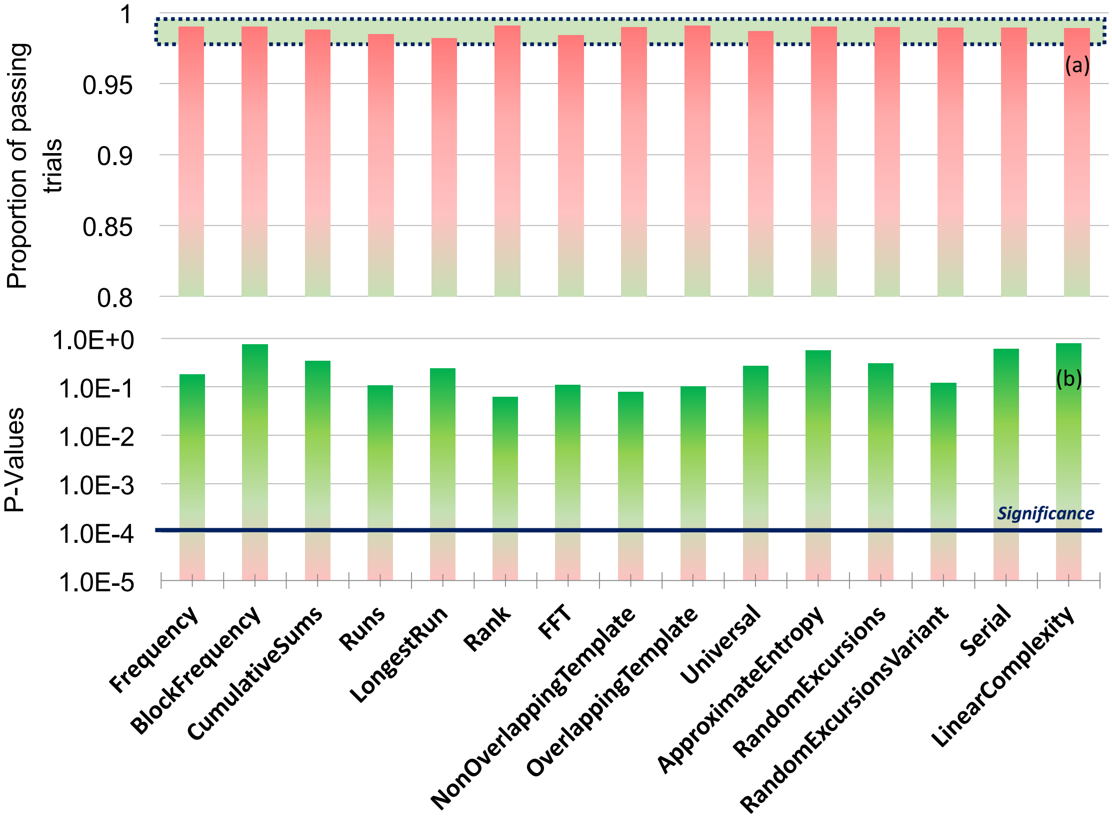


Figure C.4: Results of the NIST tests applied to 1.25 Gbits of random bits. (a) The proportion of passes of each test for 1000 1-Mb-long samples. All tests are passed with a proportion value greater than 0.9806 and less than 0.9994; (b) the P-values of each individual test, obtained from the distribution of P-values of each of the 1000 trials. All tests are passed with 1000 1-Mb-long samples and at a significance level of 0.0001. For the tests, which produce multiple P-values and proportions, the worst cases are given.

Bibliography

[1] C. H. Bennett and G. Brassard, In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing **175**, 8(1984).

[2] N. Metropolis and S. Ulam, **44**, 335(1949).

[3] B. Schneier and P. Sutherland, (John Wiley & Sons, 1995).

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145(2002).

[5] N. Gisin and R. Thew, Nature Photonics **1**, 165(2007).

[6] H.-K. Lo, M. Curty, and K. Tamaki, Nature Photonics **8**, 595(2014).

[7] H. Schmidt, Journal of Applied Physics **41**, 462(1970).

[8] H.-C. Miguel and G.-E. Juan, arXiv:1604.03304v1, quant-ph(2016).

[9] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, npj Quantum Information **2**, 16021(2016).

[10] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675(2000).

[11] M. J. Applegate, O. Thomas, J. F. Dynes, Z. L. Yuan, D. A. Ritchie, and A. J. Shields, Appl. Phys. Lett. **107**, 071106(2015).

[12] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **93**, 031109(2008).

[13] M. A. Wayne and P. G. Kwiat, Optics Express **18**, 9351(2010).

[14] H. Furst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, Optics Express **18**, 13029(2010).

[15] M. Wahl, M. Leifgen, M. Berlin, T. Rhlicke, H.-J. Rahn, and O. Benson, Appl. Phys. Lett. **98**, 171105(2011).

[16] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, Phys. Review X **4**, 031056(2014).

[17] A. Martin, B. Sanguinetti, C. C. W. Lim, R. Houlmann, and H. Zbinden, Journal of Lightwave Technology **33**, 2855(2015).

[18] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Phys. Rev. X **6**, 011020(2016).

[19] S. Pironio, A. Acin, S. Massar, A. B. Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature **464**, 1021(2010).

[20] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Phys. Rev. Lett. **114**, 150501(2015).

[21] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, Optics Lett. **35**, 312(2010).

[22] H. Guo, W. Tang, Y. Liu, and W. Wei, Phys. Rev. E **81**, 051137(2010).

[23] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, Rev. Sci. Instrum. **86**, 063105(2015).

[24] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Optics Express **20**, 12366(2012).

[25] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, Nature Photonics **4**, 711(2010).

[26] Y. Shi, B. Chng, and C. Kurtsiefer, Appl. Phys. Lett. **109**, 041101(2016).

[27] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, Nature Photonics **2**, 728(2008).

[28] A. Marandi, N. C. Leindecker, K. L. Vodopyanov, and R. L. Byer, Optics Express **20**, 19322(2012).

[29] T. Symul, S. M. Assad, and P. K. Lam, Appl. Phys. Lett. **98**, 231103(2011).

[30] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, Optics Express **19**, 20665(2011).

[31] C. Abellán, W. Amaya, D. Mitrani, V. Pruneri, and M.-W. Mitchell, Phys. Rev. Lett. **115**, 250403(2015).

[32] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acn, J. Capmany, V. Pruneri, and M. W. Mitchell, Optics Express **22**, 1645(2014).

[33] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Frhlich, A. Plews, and A. J. Shields, Appl. Phys. Lett. **104**, 261112(2014).

[34] K. Y. Lau, Appl. Phys. Lett. **52**, 257(1988).

[35] S.-H. Sun, F. Xu, M.-S. Jiang, X.-C. Ma, H.-K. Lo, and L.-M. Liang, Phys. Rev. A **92**, 022304(2015).

[36] L. C. Comandar, M. Lucamarini, B. Frhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam,Z. L. Yuan, R. V. Penty, and A. J. Shields, Nature Photonics, doi:10.1038/nphoton.2016.50(2016).

[37] N. Nisan and A. Ta-Shma, J. Comput. Syst. Sci. **58**, 148(1999).

[38] A. Rukhin, et al., (Special Publication 80022 Revision 1, National Institute of Standards and Technology, 2008).

[39] C. Abellán, W. Amaya, D. Domenech, P. Muñoz, J. Capmany, S. Longhi, M. Mitchell, and V. Pruneri, arXiv:1609.03255v1, quant-ph(2016).

[40] Our scheme employs laser pulses of a few tens of picoseconds length, created at 250 MHz without applying a current bias to the laser diode. In contrast, C. Abellán et al. use five nanosecond-long laser pulses created by superimposing a 10 mA bias current with a 100 MHz current modulation. In addition to different pulse generation rates, it is conceivable that the phase correlations between subsequent pulses are not the same in the two schemes. We furthermore note that C. Abellán et al. assessed the entropy of their source, but did not actually generate random bits and test their quality.

Appendix D

Paper IV

Quantum teleportation across a metropolitan fibre network

Nature Photonics, 10, 676680

19 September 2016

R. Valivarthi[1†], M. Grimau Puigibert[1†], Q. Zhou[1†], G. H. Aguilar[1†], V. B. Verma[2], F. Marsili[3], M. D. Shaw[3], S. W. Nam[2], D. Oblak[1] and W. Tittel[1]

[1]*Institute for Quantum Science and Technology, and Department of Physics & Astronomy, University of Calgary, 2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada*

[2]*National Institute of Standards and Technology, Boulder, Colorado 80305, USA*

[3]*Jet Propulsion Laboratory, California Institute of Technology, 4800 Oak Grove Drive, Pasadena, California 91109, USA*

†*: these authors contributed equally to this work*

Abstract

If a photon interacts with a member of an entangled photon pair via a Bell-state measurement (BSM), its state is teleported over principally arbitrary distances onto the pair's second member [2]. Since 1997, this puzzling prediction of quantum mechanics

has been demonstrated many times [2]; however, with two exceptions [3, 44], only the photon that received the teleported state, if any, travelled far while the photons partaking in the BSM were always measured closely to where they were created. Here, using the Calgary fibre network, we report quantum teleportation from a telecom-photon at 1532 nm wavelength, interacting with another telecom-photon after both have travelled several kilometres and over a combined bee-line distance of 8.2 km, onto a photon at 795 nm wavelength. This improves the distance over which teleportation takes place to 6.2 km. Our demonstration establishes an important requirement for quantum repeater-based communications [5] and constitutes a milestone towards a global quantum internet [6].

D.0.1 Introduction

While the possibility to teleport quantum states, including the teleportation of entangled states, has been verified many times using different physical systems (see Ref. [[2]] for a recent review), the maximum distance over which teleportation is possible — which we define to be the spatial separation between the BSM and the photon, at the time of this measurement, that receives the teleported state — has so far received virtually no experimental attention. (See the Supplementary Information for a motivation of this arguably most natural definition and for a description of various experiments in its light). To date, only two experiments have been conducted in a setting that resulted in a teleportation distance that exceeds the laboratory scale [3, 44], even if in a few demonstrations the bee-line distance travelled by the photon that receives the teleported state has been much longer [7, 8].

The reason to stress the importance of distances is linked to the ability of exploiting teleportation in various quantum information applications. One important example is the task of extending quantum communication distances using quantum repeaters [5], most of which rely on the creation of light-matter entanglement, e.g. by creating an entangled two-photon state out of which one photon is absorbed by a quantum memory for light [9], and entanglement swapping [10]. The latter shares the Bell state measurement (BSM) with standard teleportation; however, the photon carrying the state to be teleported is itself a member of an entangled pair. Entanglement swapping is therefore sometimes referred-to as teleportation of entanglement. To be useful in such a repeater, two entangled photon pairs must be created far apart, and the BSM, which heralds the existence of the two partaking photons and hence of the remaining members of the two pairs, should, for optimal performance, take place approximately halfway in-between these two locations.

Yet, due to the difficulty to guarantee indistinguishability of the two interacting photons after their transmission through long and noisy quantum channels [12], entanglement swapping or standard teleportation in the important midpoint configuration has only been reported very recently outside the laboratory [44]. This work exploited the heralding nature of the BSM for the first loophole-free violation of a Bell inequality — a landmark result that exemplifies the importance of this configuration. However, the two photons featured a wavelength of about 637 nm, which, due to high loss during transmission through optical fibre, makes it impossible to extend the transmission distance to tens, let alone hundreds, of kilometers. In all other demonstrations, either the travel distances of the two photons were small, or they were artificially increased using fibre on spool [3, 12, 13, 39, 40], effectively increasing travel time and transmission loss — and hence decreasing communication rates — rather than real separation. Here we report the first demonstration of quantum teleportation over several kilometers in the mid-point configuration and with photons at telecommunication wavelength.

D.0.2 Measurement and results

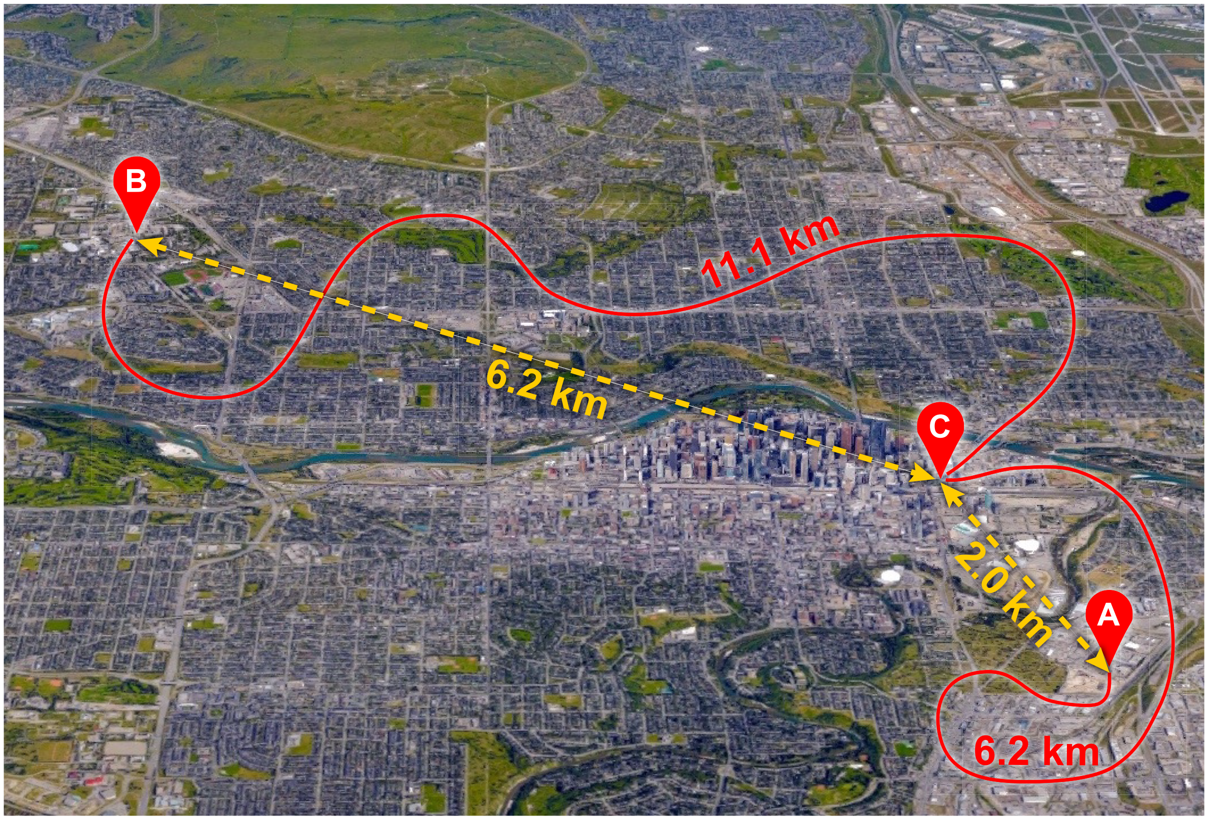


Figure D.1: **Aerial view of Calgary.** Alice 'A' is located in Manchester, Bob 'B' at the University of Calgary, and Charlie 'C' in a building next to City Hall in Calgary downtown. The teleportation distance — in our case the distance between Charlie and Bob — is 6.2 km. All fibres belong to the Calgary telecommunication network but, during the experiment, they only carry signals created by Alice, Bob or Charlie and were otherwise "dark".

An aerial map of Calgary, identifying the locations of Alice, Bob and Charlie, is shown in Fig. D.1, and Fig. E.5 depicts the schematics of our experimental setup. Alice, located in Manchester (a Calgary neighbourhood), prepares phase-randomized attenuated laser pulses at 1532 nm wavelength with different mean photon numbers $\mu_{\mathrm{A}} \ll 1$ in various time-bin qubit states $|\psi\rangle_A = \alpha |e\rangle + \beta e^{i\phi} |\ell\rangle$, where $|e\rangle$ and $|\ell\rangle$ denote early and late temporal modes, respectively, ϕ is a phase-factor, and α and β are real numbers that satisfy

$\alpha^2 + \beta^2 = 1$. Using 6.2 km of deployed fibre, she sends her qubits to Charlie, who is located 2.0 km away in a building next to Calgary City Hall. Bob, located at the University of Calgary (UofC) 6.2 km from Charlie, creates pairs of photons — one at 1532 nm and one at 795 nm — in the maximally time-bin entangled state $|\phi^+\rangle = 2^{-1/2}(|e,e\rangle + |\ell,\ell\rangle)$. He sends the telecommunication-wavelength photons through 11.1 km of deployed fibre to Charlie, where they are probabilistically projected jointly with the photons from Alice onto the maximally entangled state $|\psi^-\rangle = 2^{-1/2}(|e,\ell\rangle - |\ell,e\rangle)$. As we show in the Supplementary Information, this leads to the 795 nm wavelength photon at Bob acquiring the state $|\psi\rangle_B = \sigma_y |\psi\rangle_A$, where σ_y is the Pauli operator describing a bit-flip combined with a phase-flip. In other words, Charlie's measurement results in the teleportation of Alice's photon's state, modulo a unitary transformation, over 6.2 km distance onto Bob's 795 nm wavelength photon.

To confirm successful quantum teleportation, Bob then performs a variety of projective measurements on this photon, whose outcomes, conditioned on a successful BSM at Charlie, are analyzed using different approaches (see the Methods section for more information on how data is taken). We point out that the 795 nm wavelength photons are measured prior to the BSM, thus realizing a scenario where teleportation is achieved *a posteriori* [16, 17].

The main difficulty in long-distance quantum teleportation is to ensure the required indistinguishability (in spectral, temporal, spatial, and polarization degrees of freedom) between the two photons subjected to the BSM at Charlie (which, in our case, are only 70 ps long) despite them being created by independent sources and having travelled over several kilometres of deployed fibre. As we show in Fig. D.3, varying environmental conditions during the measurements significantly impact the polarization and arrival times of the photons. Thus, quantum teleportation is only possible with active and automated stabilization of the polarization and of the path-length difference. For the former we employ a polarization tracker and for the latter we use a novel approach based on Hong-Ou-Mandel quantum interference (see the Methods and Supplementary Information for details).

To verify successful teleportation, first, Alice creates photons in an equal superposition of $|e\rangle$ and $|\ell\rangle$ with a fixed phase, and Bob makes projection measurements onto states described by such superpositions with various phases. Conditioned on a successful BSM at Charlie's, we find sinusoidally varying triple-coincidence count rates with a visibility of $(38 \pm 4)\%$ and an average of 17.0 counts per minute. This result alone already represents a strong indication of quantum teleportation: assuming that the teleported state is a statistical mixture of a pure state and white noise, the visibility consistent with the best classical strategy and assuming Alice creates single photons is 1/3 [50]. However, here we use this result merely to establish absolute phase references for Alice's and Bob's interferometers (see the Supplementary Information).

Being able to control the absolute phase values, we can now create photons in, and project them onto, well defined states, e.g. $|e\rangle$, $|\ell\rangle$, $|\pm\rangle \equiv 2^{-1/2}(|e\rangle \pm |\ell\rangle)$, and $|\pm i\rangle \equiv 2^{-1/2}(|e\rangle \pm i\,|\ell\rangle)$. This allows us to reconstruct the density matrices ρ_{out} of various quantum states after teleportation, and, in turn, calculate the fidelities $F = {}_{\text{B}}\langle\psi|\,\rho_{\text{out}}\,|\psi\rangle_{\text{B}}$ with the expected states $|\psi\rangle_{\text{B}}$. The results, depicted in Figs. D.4 and D.5, show that the fidelity for all four prepared states exceeds the maximum classical value of 2/3 [50]. In particular, the average fidelity $\langle F\rangle = \left[F_e + F_l + 2(F_+ + F_{+i})\right]/6 = (78{\pm}1)\%$ violates this threshold by 12 standard deviations.

One may conclude that this result shows the quantum nature of the disembodied state transfer between Charlie and Bob. However, strictly speaking, the 2/3 bound only applies to Alice's state being encoded into a single photon, while our demonstration, as others before, relied on attenuated laser pulses. To extract the appropriate experimental value, we therefore take advantage of the so-called decoy-state method, which was

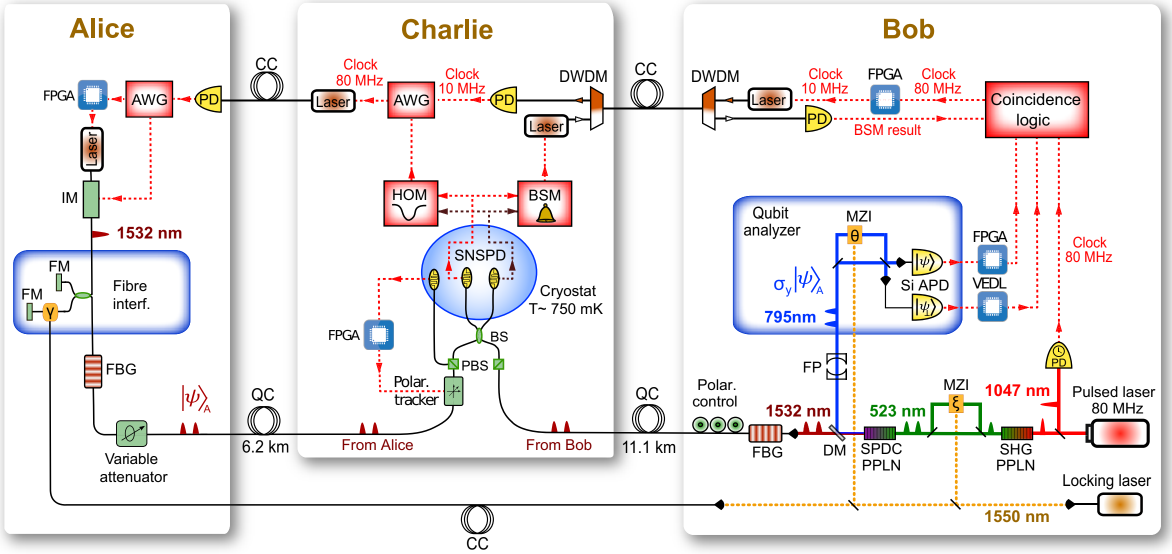


Figure D.2: **Schematics of the experimental setup. a,** Alice's setup: An intensity modulator (IM) tailors 20 ps-long pulses of light at an 80 MHz rate out of 10 ns-long, phase randomized laser pulses at 1532 nm wavelength. Subsequently, a widely unbalanced fibre interferometer with Faraday mirrors (FM), active phase control (see the Methods sections) and path-length difference equivalent to 1.4 ns travel time difference creates pulses in two temporal modes or bins. Following their spectral narrowing by means of a 6 GHz wide fibre Bragg grating (FBG) and attenuation to the single-photon level the time-bin qubits are sent to Charlie via a deployed fibre — referred to as a quantum channel (QC) — featuring 6 dB loss. **b**, Bob's setup: Laser pulses at 1047 nm wavelength and 6 ps duration from a mode-locked laser are frequency doubled (SHG) in a periodically poled lithium-niobate (PPLN) crystal and passed through an actively phase–controlled Mach-Zehnder interferometer (MZI) that introduces the same 1.4 ns delay as between Alice's time-bin qubits. Spontaneous parametric down-conversion (SPDC) in another PPLN crystal and pump rejection using an interference filter (not shown) results in the creation of time-bin entangled photon-pairs [7] at 795 and 1532 nm wavelength with mean probability μ_{SPDC} up to 0.06. The 795 nm and 1532 nm (telecommunication-wavelength) photons are separated using a dichroic mirror (DM), and subsequently filtered to 6 GHz by a Fabry-Perot (FP) cavity and an FBG, respectively. The telecom photons are sent through deployed fibre featuring 5.7 dB loss to Charlie, and the state of the 795 nm wavelength photons is analyzed using another interferometer — again introducing a phase-controlled travel-time difference of 1.4 ns — and two single photon detectors based on Silicon avalanche photodiodes (Si-APD) with 65% detection efficiency. **c,** Charlie's setup: A beamsplitter (BS) and two WSi superconducting nanowire single photon detectors [22] (SNSPD), cooled to 750 mK in a closed-cycle cryostat and with 70% system detection efficiency, allow the projection of bi-photon states — one from Alice and one from Bob — onto the $|\psi^-\rangle$ Bell state. To ensure indistinguishability of the two photons at the BSM, we actively stabilize the photon arrival times and polarization, the latter involving a polarization tracker and polarizing beamsplitters (PBS), as explained in the Methods. Various synchronization tasks are performed through deployed fibres, referred to as classical channels CC, and aided by dense-wavelength division multiplexers (DWDM), photo-diodes (PD), arbitrary waveform generators (AWG), and field-programmable gate-arrays (FPGA), with details in the Methods.

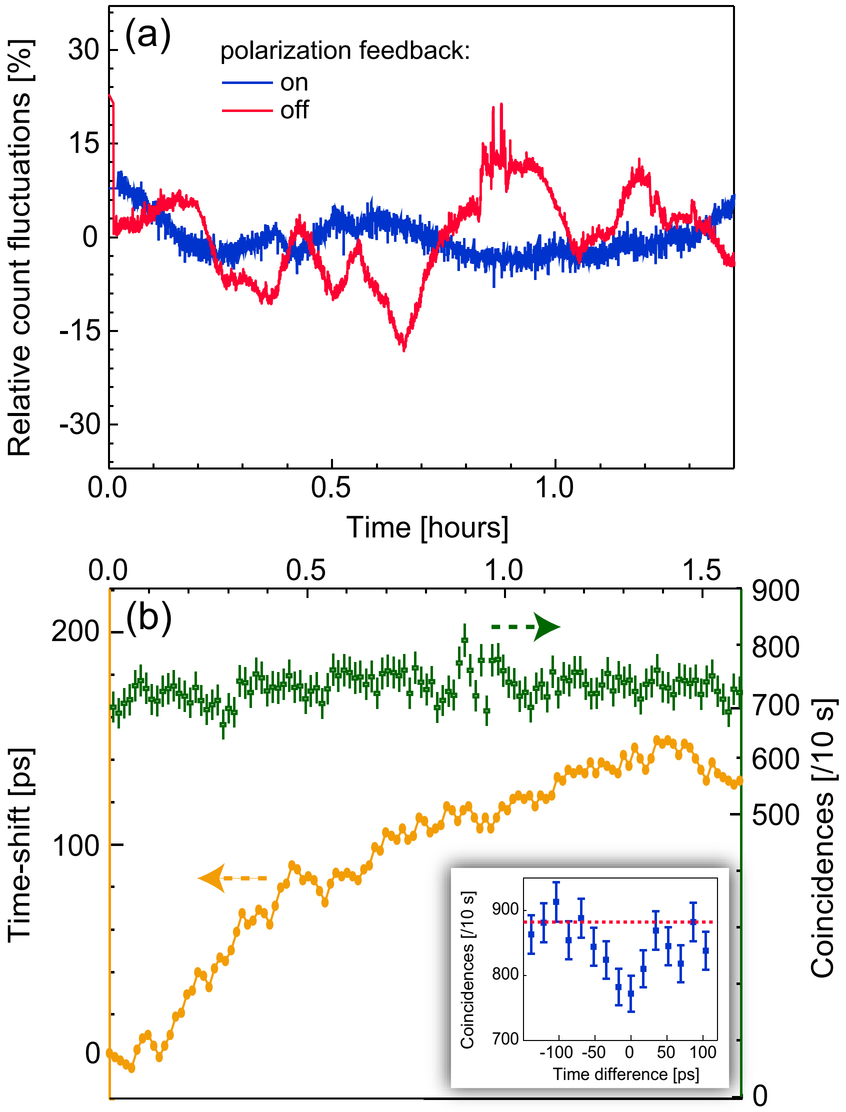


Figure D.3: **Indistinguishability of photons at Charlie. a**, Fluctuations of the count rate of a single SNSPD at the output of Charlie's BS with and without polarization feedback **b**, Inset: rate of coincidences between counts from SNSPDs as a function or arrival time difference, displaying a Hong-Ou-Mandel (HOM) dip [45] when photon-arrival times at the BS are equal. Orange filled circles: The change in the generation time of Alice's qubits that is applied to ensure they arrive at Charlie's BSM at the same time as Bob. Green empty squares: Coincidence counts per 10 s with timing feedback engaged, showing locking to the minimum of the HOM dip (see Methods and Supplementary Information for details). All error bars (one standard deviation) are calculated assuming Poissonian detection statistics.

developed for quantum key distribution (QKD) to assess an upper bound on the error rate introduced by an eavesdropper on single photons emitted by Alice [20,48]. Here, we rather use it to characterize how a quantum channel — in our case the concatenation of the direct transmission from Alice to Charlie and the teleportation from Charlie to Bob — impacts on the teleportation fidelity of quantum states encoded into individual photons [37]. Towards this end, we vary the mean number of photons per qubit emitted at Alice between three optimized values, $\mu_{\mathrm{A}} \in \{0, 0.014, 0.028\}$, and measure error rates and transmission probabilities for each value independently (see the Supplementary Information for details of how to extract the single-photon fidelity from these measurements). The results, also depicted in Fig. D.5, show again that the fidelities for all tested states exceed the maximum value of 2/3 achievable in classical teleportation. We note the good agreement between the measured values and those predicted by our model (described in the Supplementary Information), which takes into account various, independently characterized system imperfections (no fit). This allows us to identify that deviations of the measured fidelities from unity — i.e. from ideal teleportation — are mostly due to remaining distinguishability of the two photons subjected to the BSM at Charlie, followed by multi-pair emissions by the pair-source. Finally, by averaging the single-photon fidelities over all input states, weighted as above, we find $\langle F^{(1)} \rangle \geq (80 \pm 2)\%$ — as before significantly violating the threshold between classical and quantum teleportation.

D.0.3 Discussion and conclussions

Our measurements establish the possibility for quantum teleportation over many kilometres in the important mid-point configuration — as is required for extending the distance of quantum communications using quantum repeaters. We emphasize that both photons travelling to Charlie are at telecommunication wavelength, making it possible

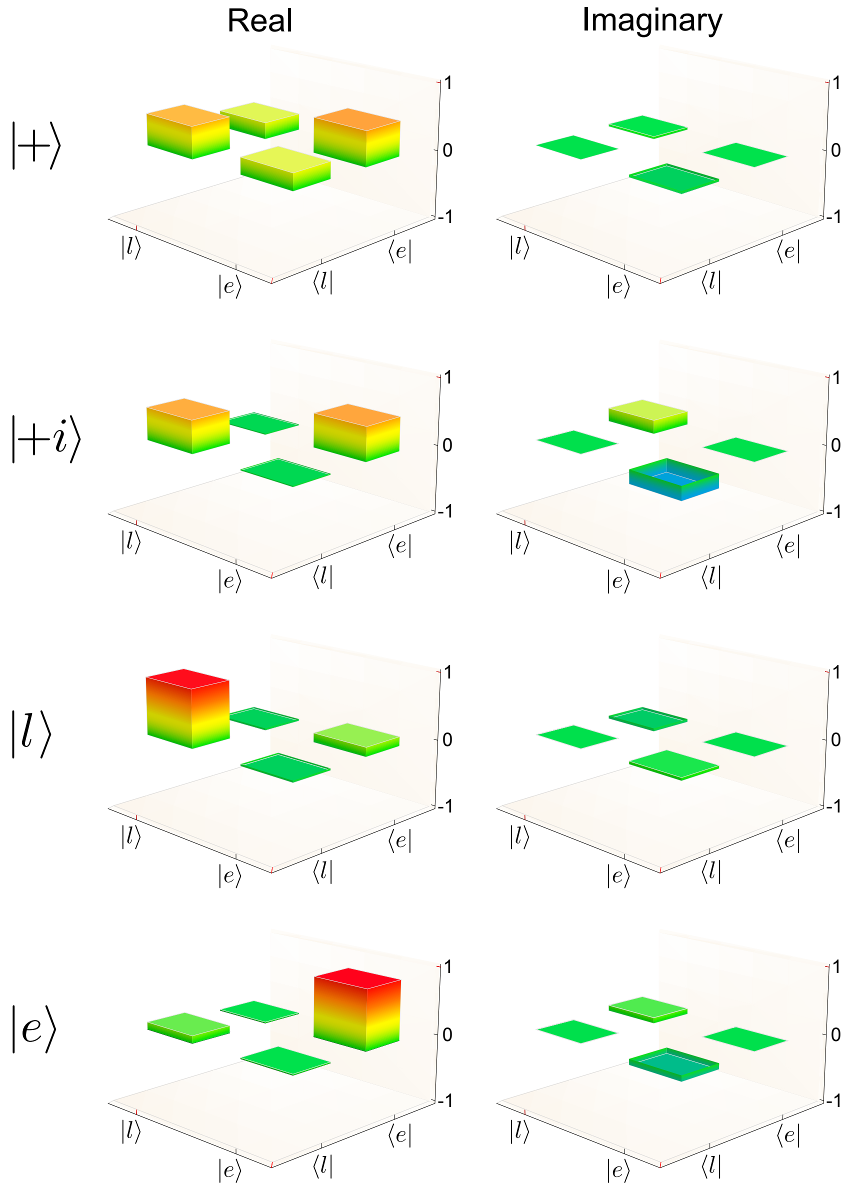


Figure D.4: **Density matrices of four states after teleportation.** Shown are the real and imaginary parts of the reconstructed density matrices for four different input states created at Alice. The mean photon number per qubit is $\mu_{\mathrm{A}} = 0.014$, and the mean photon pair number is $\mu_{\mathrm{SPDC}} = 0.045$. The state labels denote the states expected after teleportation.

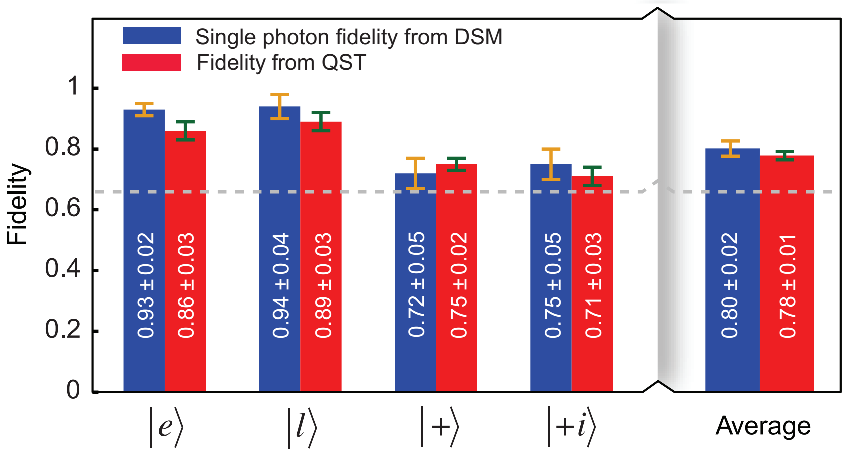


Figure D.5: Individual and average fidelities of four teleported states with expected (ideal) states, measured using quantum state tomography (QST) and the decoy-state method (DSM). For the DSM we set $\mu_{\text{SPDC}} = 0.06$. Error bars (one standard deviation) are calculated assuming Poissonian detection statistics and using Monte-Carlo simulation. Count rates for both methods are provided in the Supplementary Information. The somewhat larger degradation of $|+\rangle$ and $|+i\rangle$ states is due to the limited quality of the BSM (see Supplementary Information) and imperfect interferometers. Neither cause an effect for $|e\rangle$ and $|l\rangle$ states.

to extend the Alice-Bob distance from its current value of 8 kilometres by at least one order of magnitude. This corresponds to the distance of an elementary link, which includes teleportation of entanglement, at which communication links based on spectrally multiplexed quantum repeaters start to outperform direct qubit transmission [25, 37].

We also note that the 795 nm photon, both in terms of central wavelength as well as spectral width, is compatible with quantum memory for light — a key element of a quantum repeater — in cryogenically-cooled thulium-doped crystals [26]. This, in conjunction with projection onto two Bell states [27], would allow us to implement active feed-forward on the teleported photon. An interesting question is if our implementation - in particular the laser used to stabilize the phase in Alices and Bobs interferometers - opens side channels for eavesdropping. While this topic is beyond the scope of our investigation, we emphasize that lasers with sufficient stability to allow for local (independent) stabilization are available [28].

Finally, we point out that quantum teleportation involves the interesting aspect of Alice transferring her quantum state in a disembodied fashion to Bob without him ever receiving any physical particle. In other words, Bob is only sending photons (all of them members of an entangled pair) and thus better able to protect his system from any outside interference, e.g. from an adversary [29].

We note that, a related experimental demonstration has been reported in a concurrent manuscript [30].

Acknowledgments

The authors thank Tyler Andruschak and Harpreet Dhillon from the City of Calgary for providing access to the fibre network and for help during the experiment, Vladimir Kiselyov for technical support, and Pascal Lefebvre for help with aligning the entangled photon pair source. This work was funded through Alberta Innovates Technology Futures (AITF), the National Science and Engineering Research Council of Canada (NSERC), and the Defense Advanced Research Projects Agency (DARPA) Quiness program (contract no. W31P4Q-13-l-0004). WT furthermore acknowledges funding as a Senior Fellow of the Canadian Institute for Advanced Research (CIFAR), and VBV and SWN acknowledge partial funding for detector development from the Defense Advanced Research Projects Agency (DARPA) Information in a Photon (InPho) program. Part of the detector research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

Author contributions

The SNSPDs were fabricated and tested by VBV, FM, MDS, and SWN. The experiment was conceived and guided by WT. The setup was developed, measurements were performed and the data analyzed by RV, MGP, QZ, GHA, and DO. The manuscript was written by WT, RV, MGP, QZ, GHA, and DO.

Additional information

Supplementary information is available in the online version of the paper. * Correspondence and requests for materials should be addressed to W. Tittel (email: wtittel@ucalgary.ca).

Competing finantial interests

The authors declare no competing financial interests.

D.0.4 Methods

Synchronization

For the following discussion, please refer to experimental setup outlined in Fig. E.5. Charlie is connected via pairs of optical fibres both to Alice and to Bob. In each pair, one fibre — referred to as the quantum channel (QC) — carries single photons, while the other — referred to as the classical channel (CC) — distributes various strong optical signals whose purpose will be described in the following. In addition, Alice and Bob are directly connected via an optical fibre that transmits narrow-line-width laser light at 1550 nm in order to lock the phases of all interferometers , i.e. γ, ξ and θ shown in Fig. E.5. This is crucial for maintaining a common phase reference for the qubit states generated at Alice and Bob, and analyzed at Bob. In each interferometer, the power of the locking laser in one output arm (measured on a classical detector) is used to derive a feedback signal to a piezo-element that regulates the path-length difference of the interferometer to maintain a fixed phase. For instance, for free-space-optics-based interferometers at Bob, the path-length difference is changed by moving a mirror with the piezo stack, while for the fibre-optics interferometer at Alice, the path-length is adjusted by stretching a fibre wrapped around a piezo-tube. Additionally, all interferometers are kept in temperature-controlled boxes.

The master clock for all devices is derived from detection of the mode-locked laser pulses (80 MHz) and converted back into an optical signal for distribution through the CC via Charlie to Alice.

Stabilization to ensure photon indistinguishability

For a successful BSM, the photons arriving at Charlie from Alice and Bob need to be indistinguishable despite being generated by independent and different sources, and having travelled through several kilometres of deployed fibre. The spatial indistinguishability is naturally ensured by the propagation in single-mode optical fibres. To ensure that the photons have the same spectral profile, they are sent through separate, temperature-stabilized fibre Bragg gratings (FBG) that narrow their spectra to 6 GHz. The spectral overlap of the FBGs at Alice and Bob needs to be set only once. However, due to temperature-dependent properties of fibre such as birefringence and length, the polarization and arrival time of the photons change with external environmental conditions, making it difficult to implement the BSM in a real-world environment. Towards this end, we apply feedback mechanisms to compensate for drifts in polarization and arrival time.

Timing

The short duration of our photons (70 ps) prevents us from using the SNSPDs (featuring a time jitter of ∼150 ps) to directly determine their arrival times with the required precision to adjust the difference to zero. Instead, we compensate for arrival-time drifts with the novel approach of observing the degree of quantum-interference (Hong-Ou-Mandel or HOM effect [45]) of the photons. The signals from the two SNSPDs (which are used to perform the BSM) are also sent to a HOM analyzing unit (see Fig. E.5) that monitors the number of coincidences between detections corresponding to either both photons arriving in an early time bin mode, or both in a late bin. As shown in the inset of Fig. D.3b, the HOM interference causes photon bunching and thus the coincidences to be reduced when the photons arrive at the beam splitter at the same time. Hence, to counteract the drift in travel time of the photons, we vary the qubit generation time at Alice with a precision of about ∼4 ps to keep the coincidence count rate at the minimum value of around 750 per 10 sec., as shown in Fig. D.3b. In practice Alice's time-shift is triggered at Charlie by shifting the phase of the master clock signal that he forwards to Alice. Fig. D.3b, shows that, during a typical 1.5 hour measurement, we apply a time shift of ∼200 ps to compensate drifts in timing. Since the shift is larger than the duration of the photons, the teleportation protocol would fail without the active stabilization.

Polarization

Because photons from Alice and Bob pass through polarizing beam-splitters (PBS) at Charlie, their polarization indistinguishability is naturally satisfied. However, correct photon polarizations must be set and maintained to maximize the transmission through the PBSs, or else the channel loss will vary over time. In our system, the QC between Bob and Charlie experiences only a slow drift, which allows for manual compensation using a polarization controller — located at Bob — once a day. However, an automated polarization feedback system is required for the channel between Alice and Charlie, which drifts significantly on the time-scale of the experiment. To that end, we monitor the count rate of an additional SNSPD, located in the reflection port of the PBS at Charlie, with a field-programmable gate-array (FPGA) so as to generate a feedback signal that minimizes the rate by adjusting the polarization by means of a polarization tracker (also located at Charlie). As seen in Fig. D.3, the intensity fluctuations in 1.5 hours (a typical time scale to acquire results for one qubit setting) are limited to 5% with feedback, and to about 15% without feedback.

Data collection

Using Alice's qubits and the 1532 nm-members of the entangled pairs, Charlie performs $|\psi^-\rangle$ Bell-state projections. Such a projection occurs when one SNSPD detects a photon arriving in the early time-bin and the other SNSPD records a photon in the late time-bin. Successful Bell-state projection measurements are communicated via the CC and using classical laser pulses to Bob, who converts them back to electrical signals. Each signal is then used to form a triple coincidence with the detection signal of the 795 nm wavelength photon exiting Bob's qubit analyzer. Towards this end, the latter is delayed using a variable electronic delay-line (VEDL) implemented on an FPGA by the time it takes the 1532 nm entangled photon to travel from Bob to Charlie plus the travel time of the BSM signal back to Bob.

D.0.5 Supplementary information

Teleportation protocol

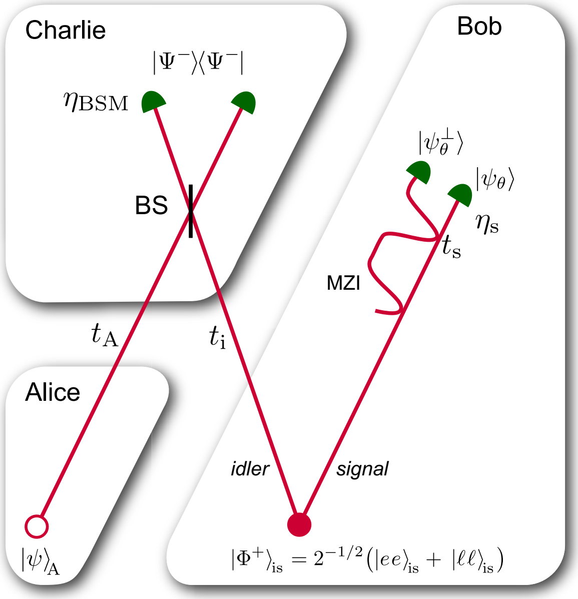

Charlie
$|\Psi^-\rangle\langle\Psi^-|$
η_{BSM}
BS
t_{A}
t_{i}
Alice
$|\psi\rangle_{\mathrm{A}}$
Bob
$|\psi_\theta^\perp\rangle$
$|\psi_\theta\rangle$
η_{s}
t_{s}
MZI
idler
signal
$|\Phi^+\rangle_{\mathrm{is}} = 2^{-1/2}(|ee\rangle_{\mathrm{is}} + |\ell\ell\rangle_{\mathrm{is}})$

Figure D.6: Schematics of the teleportation experiment. Alice encodes time-bin qubits $|\psi\rangle_{\mathrm{A}}$ using attenuated laser pulses with mean photon number μ_{A} and sends them to Charlie. Bob prepares photon pairs in the maximally entangled time-bin qubit state $|\Phi^+\rangle_{\mathrm{is}}$ with mean photon number μ_{SPDC} and sends the 'idler' member of each photon pair to Charlie. Charlie interferes the photons he receives from Alice and Bob on a beam-splitter and probabilistically projects them onto the Bell-state $|\Psi^-\rangle_{\mathrm{Ai}}$. This results in Bob's 'signal' photons acquiring the state $|\psi\rangle_{\mathrm{s}} = \sigma_y\,|\psi\rangle_{\mathrm{A}}$. The 'signal' photons are then sent to a time-bin qubit analyzer which allows projections onto two orthogonal states (here $|\psi_\theta\rangle$ and $|\psi_\theta^\perp\rangle = |\psi_{(\theta+\pi)}\rangle$ where θ is the phase-difference between the two MZI arms). The transmission probabilities of the three channels are labelled as t_{c}, t_{i} and t_{s}, and η_{BSM}, η_{s} are the efficiencies of the employed detectors.

In this section we will briefly outline the steps in our teleportation protocol. In Supplementary Figure D.6, we show a typical schematic of the teleportation experiment. The quantum teleportation protocol [2] can be described as follows:

1. Bob prepares a maximally time-bin entangled two-photon state $|\Phi^+\rangle_{\mathrm{is}} = 2^{-1/2}(|e,e\rangle_{\mathrm{is}} + |\ell,\ell\rangle_{\mathrm{is}})$, where s and i denote the 'signal' and 'idler' photons from the spontaneous parametric down conversion process (SPDC), and $|e\rangle$ and $|\ell\rangle$ denote early and late temporal modes (or bins), respectively.

2. Alice prepares an arbitrary time-bin qubit encoded into two temporal modes of an attenuated laser pulse. It can be written as $|\psi\rangle_{\mathrm{A}} = \alpha\,|e\rangle_{\mathrm{A}} + \beta e^{i\phi}\,|\ell\rangle_{\mathrm{A}}$, where ϕ is the relative phase between the two temporal modes, α and β are real, and $\alpha^2+\beta^2=1$.

3. Charlie receives the 'idler' photon of the entangled pair from Bob, and the photon from Alice. He then probabilistically projects the state of these photons onto one of the four Bell-states (in our experiment $|\Psi^-\rangle_{\mathrm{Ai}}$, defined below). This is known as a Bell state measurement (BSM).

4. Conditioned on the outcome of the BSM, the 'signal' photon that is with Bob acquires the qubit state that Alice prepared her photon in, modulo a known unitary transformation U. Bob can choose to apply the unitary, $U^\dagger$ on the 'signal' photon to recover Alice's original state, or just account for the transformation when analyzing the data of the measurement that this photon was part of.

The mathematical description of the above protocol starts with the three-photon state from Bob and Alice:

$$|\Psi\rangle_{\mathrm{Ais}} = |\psi\rangle_{\mathrm{A}} \otimes |\Phi^+\rangle_{\mathrm{is}}\,. \tag{D.1}$$

Rewriting this state in terms of the four maximally entangled Bell-states of Alice's and the 'idler' photon, defined as $|\Phi^\pm\rangle_{\mathrm{Ai}} = 2^{-1/2}(|e,e\rangle_{\mathrm{Ai}}\pm|\ell,\ell\rangle_{\mathrm{Ai}})$ and $|\Psi^\pm\rangle_{\mathrm{Ai}} = 2^{-1/2}(|e,\ell\rangle_{\mathrm{Ai}}\pm$

$\left|\ell, e\right\rangle_{\mathrm{Ai}}$), we obtain

$$
\begin{aligned}
\left|\Psi\right\rangle_{\mathrm{Ais}} =& \frac{1}{2}\Big[\left|\Phi^{+}\right\rangle_{\mathrm{Ai}} \left(\alpha \left|e\right\rangle_{\mathrm{s}} + e^{i\phi}\beta \left|\ell\right\rangle_{\mathrm{s}}\right) \\
& + \left|\Phi^{-}\right\rangle_{\mathrm{Ai}} \left(\alpha \left|e\right\rangle_{\mathrm{s}} - e^{i\phi}\beta \left|\ell\right\rangle_{\mathrm{s}}\right) \\
& + \left|\Psi^{+}\right\rangle_{\mathrm{Ai}} \left(e^{i\phi}\beta \left|e\right\rangle_{\mathrm{s}} + \alpha \left|\ell\right\rangle_{\mathrm{s}}\right) \\
& + \left|\Psi^{-}\right\rangle_{\mathrm{Ai}} \left(e^{i\phi}\beta \left|e\right\rangle_{\mathrm{s}} - \alpha \left|\ell\right\rangle_{\mathrm{s}}\right) \Big].
\end{aligned}
\tag{D.2}
$$

Since each term is equally weighted, the probability of projecting onto any of the Bell-states is 1/4. In our setup we only project onto $\left|\Psi^{-}\right\rangle_{\mathrm{Ai}}$, in which case we keep only the last term and, hence, the qubit state of the 'signal' photon reduces to

$$
\left|\psi\right\rangle_{\mathrm{s}} = e^{i\phi}\beta \left|e\right\rangle_{\mathrm{s}} - \alpha \left|\ell\right\rangle_{\mathrm{s}}. \tag{D.3}
$$

It can be seen that the unitary operator to be applied to $\left|\psi\right\rangle_{\mathrm{s}}$ in order to recover Alice's qubit is the Pauli operator σ_y — corresponding to a bit flip combined with a phase flip. That is

$$
\left|\psi\right\rangle_{\mathrm{A}} = \sigma_y \left|\psi\right\rangle_{\mathrm{s}}. \tag{D.4}
$$

Teleportation distance

In this section, first, we discuss the differences between what we call the teleportation distance and the total distance over which the quantum state travels, which we will refer to as the state-transfer distance, and relate these two distances to long distance quantum communications using quantum repeaters (QR). In particular, we describe a few important examples of teleportation experiments and identify their teleportation distance and state-transfer distances as well as the technology platform (fibre or free-space). With an eye on the practical application of the realizations, we refer to distances measured in bee-line throughout this section

The teleportation distance, as defined in the main text, is the spatial separation, at the time of the BSM, between the BSM and the photon that receives the teleported state. To motivate this definition, we first note that after the measurement of one member of an entangled pair, quantum information is transmitted quasi-instantaneously onto the second member, as was shown by the Geneva group [32] and USTC in Hefei [33]. Applied to quantum teleportation this means that at the exact time at which the BSM is performed the quantum state of Alice's photon is, almost instantaneously and without exchange of any physical entity, transferred to the other member of the entangled pair (modulo a unitary operation). For example, in the experiment categorized in Supplementary Figure D.7c), the teleportation distance would be of only a few meters. The total distance of the state-transfer, in contrast, corresponds to the spatial separation between the initial position of the photon encoding the quantum state at the time it is emitted and the final position of the photon that receives the final state at the time it is measured. In the same example, this distance is between 100 and 150 km [34, 35].

In conjunction with the above-described fundamental aspect of teleportation vs. state-transfer distance, the distinction is also important in light of long distance quantum communication based on quantum repeaters. In this application, a large teleportation distance (as per our definition) is a necessary (yet not sufficient) condition to ensure optimal performance. To elaborate, quantum repeater architectures are based on entanglement swapping (teleportation of entanglement) between an arbitrary long chain of so-called elementary links [36] from Alice to Bob. A successful BSM heralds the entanglement distribution (or swapping) between the end points of an elementary link where photons are stored until the information of the BSM is received. When entanglement has been heralded in two adjacent elementary links, either at different times or in different spectral channels, the photons at the interconnect of the two links are recalled from the quantum memory and entanglement swapping is performed over the combined distance of the two elementary links. The sequence is repeated until Alice and Bob share an entangled state.

It can be shown that the midpoint configuration, in which the BSM station is located at the middle of an elementary link as illustrated in Supplementary Figure D.7a), is required for optimal performance of a quantum repeater-based communication link – at least if the protocol in Ref. [37] is considered. This configuration minimizes the storage time in the quantum memories at the end-points of the elementary links. We conjecture that the symmetric setup (mid-point configuration) also optimizes other repeater architectures. Hence, a large teleportation distance is necessary.

In Supplementary Figure D.7, we show the space-time diagrams of different experimental implementations of quantum teleportation in which at least one of the photons travels a long distance in bee-line. Supplementary Figure D.7a) displays the diagram for the optimized elementary link of a quantum repeater based on spectral multiplexing [37]. Pairs of entangled photons are created by the sources at A and B. One of the photons from each pair is stored in a quantum memory, represented by a vertical red line. The other two photons are sent to C, where a BSM is performed. In the optimized configuration of the quantum repeater, C is at the mid-point of the link between A and B and the teleportation distance is thus half of the total distance. The diagrams in Supplementary Figure D.7b-d) show the experimental realizations of quantum teleportation over distances that exceed the laboratory scale. The diagram corresponding to our experiment is shown in Supplementary Figure D.7b): Photons and pairs of entangled photons are created at A and B, respectively. One of the photons of each pair is detected at B while the BSM is performed on the remaining photon of the pair and a photon coming from A. Hence, in our realization the teleportation distance is the distance between C and

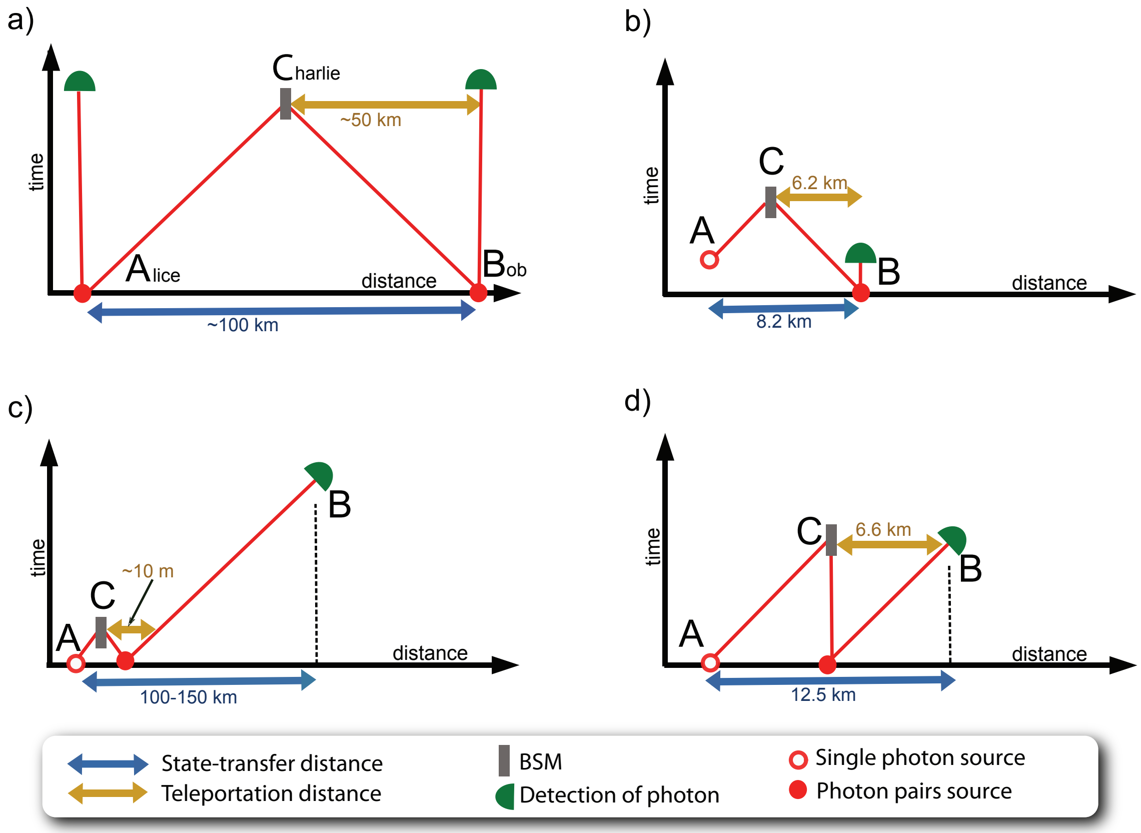


Figure D.7: **Space-time diagrams teleportation experiments. a)** Elementary link of an optimal quantum repeater [[36,37]]. **b)** Our experiment. **c)** Quantum teleportation experiments with large state-transfer distances [[34, 35]]. **d)** Experiment performed by Hefei group in concurrence with ours [[38]]. Distances or times in all panels are not to scale (they only indicate general features). For simplicity we assume the speed of light to be in air.

B (6.2 km in bee-line) and the total distance corresponds to A-B (8.2 km in bee-line). Though still somewhat asymmetric, our experimental setup thus resembles the optimal configuration for a QR. Supplementary Figure D.7c) shows the diagram corresponding to long state-transfer-distance quantum teleportation experiments over free space and fiber links implemented in the recent years [34,35]. Single photons and pairs of entangled photons are generated near each other. The BSM is performed in close proximity (we assume a lab-scale of about 10 m at most) while the other photon of each pair is transmitted over a long distance before being detected. Although the total distance over which the quantum state is transferred exceeds 100 km, the teleportation distance is very small and, as a consequence, these experiments are not useful for optimal quantum repeater architectures. In Supplementary Figure D.7d) we show the diagram for an experiment realized at the same time as ours [38]: Individual photons and pairs of entangled photons are generated at A and C, respectively. The BSM, which is situated at C, is performed on the photons from A after having travelled over 5.9 km in bee-line and one of the photons of the pair, which stayed at C in a optical fibre delay line. The other photon of each pair travels 6.6 km in bee-line before being detected. In this case, the teleportation distance is the distance between C and B (6.6 km in bee-line). While far away from a symmetric configuration, this experiment nevertheless features a a long teleportation distance. The state-transfer distance is on the order of 12.5 km in bee-line.

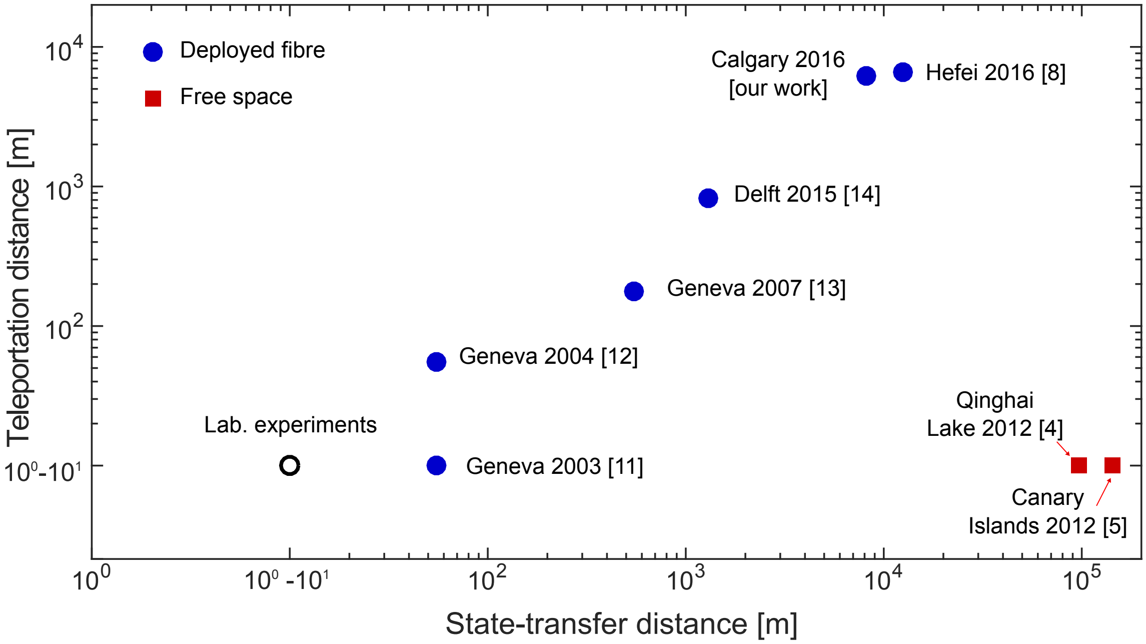


Figure D.8: **Teleportation distance vs. total quantum state-transfer distance** for different experimental implementations of quantum teleportation (all distances measured in bee-line). Black circles represent all experiments performed within a lab. Blue filled circles correspond to experiments where photons propagated through optical fibers outside a lab (deployed fibre). Red filled squares represent experiments where one photon propagates through a free-space link outside the lab.

To summarize the state-of-the-art in teleportation experiments we plot in Supplementary Figure D.8 the teleportation and state-transfer distances for different experimental implementations of quantum teleportation (all distances measured in bee-line). We can see that the longest state-transfer distances have been achieved in the demonstrations in which the photon that receives the teleported state traveled over a long distance free space [34, 35], however, the associated teleportation distances were limited to a few meters (i.e. the size of an optical table). As illustrated in Supplementary Figure D.7c), this is because the BSM was performed in proximity of both the single-photon as well as photon-pair source. A few experiments have been performed using spooled fibre [39, 40]. While being important steps towards the use of deployed fiber, teleportation distances and state-transfer distances were thus limited to a few meters in bee-line.

To conclude, please note that teleportation and state-transfer distances have steadily increased since 1998 from their original values of a few metres up to around 10 and 150 km, respectively. This gives confidence that quantum teleportation will soon meet the requirements to be useful for long distance quantum communication links based on quantum repeaters.

Estimating indistinguishability of photons at Charlie

We use Hong-Ou-Mandel (HOM) quantum interference [45] to estimate the indistinguishability of photons involved in the BSM. The HOM effect is measured by observing the number of coincidence counts between two detectors placed at each output of a beam-splitter (BS) when photons are sent into both inputs of the BS. If indistinguishable single photons are input to the BS, they will always bunch at the outputs of the BS and thus coincidences will never occur. However, if the two single photons are distinguishable, the HOM interference disappears and the photons pick outputs independently, i.e. coincidences occur half of the time. The HOM effect is quantified by the visibility, defined as

$$\mathrm{V}_{\mathrm{HOM}} = \frac{C_{\max} - C_{\min}}{C_{\max}}, \tag{D.5}$$

where $C_{\max}$ and $C_{\min}$ are the maximum and minimum coincidence counts per unit of time for the least and most indistinguishable setting achievable in an experiment, respectively. Hence, for perfectly indistinguishable single photons, $\mathrm{V}_{\mathrm{HOM}} = 1$. If instead of perfect single photons we input pulses with certain photon number statistics, the bunching is no longer perfect, but is bounded by a value that can be predicted based on the photon number distribution. For example, assuming Poissonian (thermal) distributions at both BS inputs, the visibility is bounded by $\mathrm{V}_{\mathrm{HOM}} = 1/2$ $(1/3)$. Regardless the photon-number distributions we have at the inputs, we can thus gauge the degree of indistinguishability of the photons by measuring how close the visibility is to the expected bound. In our case, we have a coherent state (with Poissonian-distributed photons) from Alice and a thermal state from Bob at the inputs of Charlie's BS. To model the behaviour of $\mathrm{V}_{\mathrm{HOM}}$, we follow a similar approach as in Ref. [46]. We find that the maximum HOM visibility in our situation depends on the mean photon number μ_{A} of Alice's attenuated laser pulses, and the mean pair number μ_{SPDC} of Bob's entangled pairs.

As shown in Supplementary Figure D.9, we gradually change the indistinguishability of the photons by changing their relative arrival time at the BS, thereby observing a HOM dip with visibility $\mathrm{V}_{\mathrm{HOM}} = 0.20$. Varying μ_{A} while keeping μ_{SPDC} constant, we then obtain the values for $\mathrm{V}_{\mathrm{HOM}}$ shown in Supplementary Figure D.10. The solid line is a fit of our model to the experimental data. From this fit, we estimate the indistinguishability of photons at Charlie to be (68 ± 2)%. We note that most of the reduction in the indistinguishability from the ideal value of 1 is due to imperfect spectral overlap as well as timing jitter caused by imperfect synchronization of the sources at Alice and Bob.

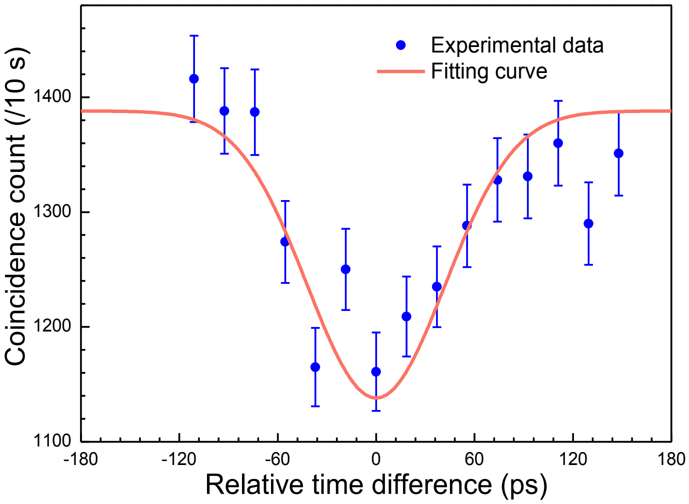


Figure D.9: A typical HOM dip in the two-fold coincidences observed in our experiment with $\mu_{\mathrm{A}} = 0.0027$ and $\mu_{\mathrm{SPDC}} = 0.03$. From the fit, we estimate the duration of the photons to be 70 ps, which is determined by the filtering bandwidth of 6 GHz.

Phase calibration of interferometers

In this section, we describe how we establish absolute phase values for the interferometers at Alice and Bob. Following the protocol described in Supplementary Section D, Alice prepares the state $|\psi\rangle_{\mathrm{A}} = 2^{-1/2}(|e\rangle_{\mathrm{A}} + e^{i\phi}\,|\ell\rangle_{\mathrm{A}})$, and, according to Eq. (D.3), the state of the 'signal' photon after a successful BSM becomes $|\psi\rangle_{\mathrm{s}} = 2^{-1/2}(|e\rangle_{\mathrm{s}} - e^{-i\phi}\,|\ell\rangle_{\mathrm{s}})$ (making use of the fact that $\alpha = \beta = 2^{-1/2}$). The two output ports of Bob's unbalanced Mach Zehnder interferometer (MZI) correspond to projections onto the states $|\psi_\theta\rangle = 2^{-1/2}(|e\rangle + e^{i\theta}\,|\ell\rangle)$ and $|\psi_\theta^\perp\rangle = 2^{-1/2}(|e\rangle - e^{i\theta}\,|\ell\rangle)$, respectively. Hence, the probability to find the photon in the first output port is

$$|\langle\psi_\theta\,|\psi\rangle_s|^2 = \frac{1}{2}\big(1 + \cos\Delta\phi\big)\ , \tag{D.6}$$

and for the second is:

$$|\langle\psi_\theta^\perp\,|\psi\rangle_s|^2 = \frac{1}{2}\big(1 - \cos\Delta\phi\big)\ , \tag{D.7}$$

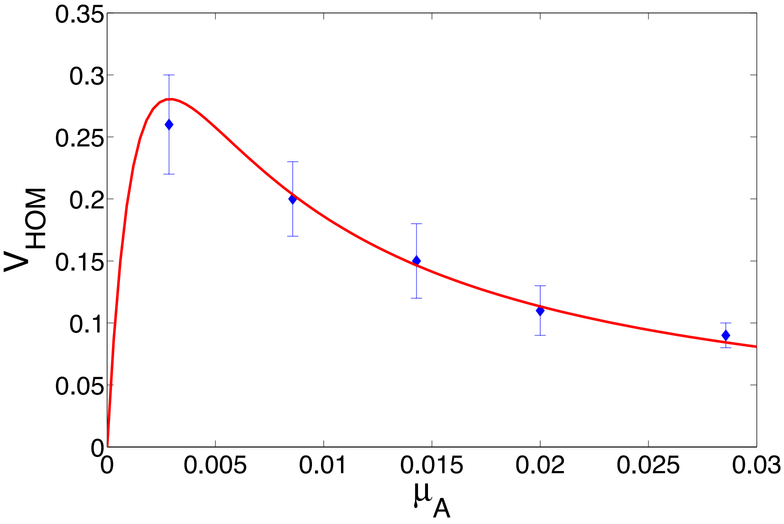


Figure D.10: Visibility of the HOM dip (V_{HOM}) versus mean photon number of Alice's laser pulses (μ_{A}). For all the measurements, $\mu_{\mathrm{SPDC}} = 0.03$.

where $\Delta\phi = \phi - \theta$. Thus, we expect the count rates at each output of Bob's MZI to show a sinusoidal dependence on ϕ (the phase of Alice's interferometer) and θ (the phase of Bob's analyzing interferometer).

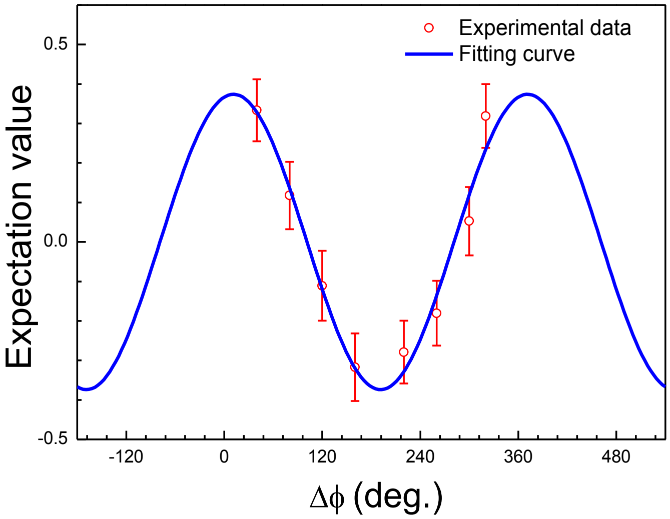


Figure D.11: Expectation value $\langle E \rangle$ as a function of the phase difference $\Delta\phi$. Circles indicate experimental data and the solid line is a sinusoidal fit. From the fit, we find a fidelity of 0.69 ± 0.02.

Because of experimental imperfections, we do not expect complete constructive and destructive interference in the MZI outputs for $\Delta\phi = \pi$, as predicted by Eqs. (D.6) and (D.7). However, conditioned on a successful BSM, we still expect to observe a sinusoidal dependence of the count rates in both output ports when varying the phase θ of the MZI.

To quantify the result, we use the expectation value

$$\langle E\rangle = \frac{C(|\psi_\theta\rangle) - C(|\psi_\theta^\perp\rangle)}{C(|\psi_\theta\rangle) + C(|\psi_\theta^\perp\rangle)}, \tag{D.8}$$

where $C(|\psi_\theta\rangle)$ $(C(|\psi_\theta^\perp\rangle))$ is the number of coincidences per unit of time in one or the other output with Bob's interferometer set to a phase θ. In the Supplementary Figure D.11 we show the expectation value $\langle E\rangle$ as a function of the phase difference $\Delta\phi$. When it reaches the maximum, we define the qubit prepared at Alice to be $|+\rangle$, and the two output ports of the MZI to correspond to projections onto $|+\rangle$ and $|-\rangle$, respectively. Recall that the entangled state prepared at Bob is $|\Phi^+\rangle_{\text{is}} = 2^{-1/2}(|e,e\rangle_{\text{is}} + |\ell,\ell\rangle_{\text{is}})$.

An additional result of this measurement is the fidelity of teleportation, which can be extracted directly from the curve as $F = [1 + max(\langle E\rangle)]/2$. From a sinusoidal fit, we obtain $F = 0.69 \pm 0.02$.

Predicting fidelities

In this section, we develop a simple model that aids our understanding of the main limiting factors in our experiment. Our model, which is inspired by that in Ref. [39], allows us to predict the measured fidelity of the teleported state conditioned on a successful BSM projection (3-fold photon coincidence detection). The model takes into account the different photon number statistics of our sources (Poissonian for Alice and thermal for Bob), the degree of indistinguishability of the photons partaking in the BSM and the total transmissions as well as the detector efficiencies.

As described in the previous section, we can set the phase θ of Bob's MZI qubit-analyzer such that for a perfect teleported state, we would observe detection events in only one of his detectors, say in the port labelled $|\psi_\theta\rangle$ (see Supplementary Figure D.6). Any detections in the other output port $|\psi_\theta^\perp\rangle$ would thus stem from a deviation of the actually teleported state $|\psi\rangle_\mathrm{s}$ from the ideal one. Such deviation may be caused by imperfections of either the initial state $|\psi\rangle_\mathrm{A}$, or of the implementation of the teleportation protocol. The fidelity of the teleported state can be estimated by measuring the probabilities of 3-fold coincidence involving Bob's detector in the desired output (P_D) as well as that for the undesired output (P_U)

$$F = \frac{P_D}{P_D + P_U}. \tag{D.9}$$

Our model allows predicting the projection probabilities P_D and P_U.

The starting point of the model is to use the knowledge of the probabilities of projecting onto $|\Psi^-\rangle_\mathrm{Ai}$ given certain combinations of photon numbers at the BS inputs. For example with a single photon at each BS input the probability to project onto $|\Psi^-\rangle_\mathrm{Ai}$ is 1/4 [see Eq. (D.2)]. Hence, we define $P(n_\mathrm{A}, n_\mathrm{i}, n_\mathrm{s})$ as the probability to detect a 3-fold coincidence (i.e. projection onto the $|\Psi^-\rangle$ Bell-state and onto *either* $|\psi_\theta\rangle$ *or* $|\psi_\theta^\perp\rangle$) in the case where n_A photons and n_i photons arrive at the beam-splitter (BS) from Alice and Bob, respectively, and n_s 'signal' photons are generated by the entangled photon pair source. It is important to note that probability $P(n_\mathrm{A}, n_\mathrm{i}, n_\mathrm{s})$ is not conditioned on having certain photon numbers at the inputs, rather it provides a means to treat the various contributions to the total 3-fold coincidence probability for separate cases, which have different probabilities to project onto $|\Psi^-\rangle_\mathrm{Ai}$. We take into account the probabilities of 3-fold coincidences for all cases in which $n_\mathrm{A} \leq 2$, $n_\mathrm{i} \leq 2$, $n_\mathrm{A} + n_\mathrm{i} \leq 2$ and $n_\mathrm{s} \leq 2$. We note that for small mean photon numbers, higher order contributions are negligible.

For instance, the probability $P(1_\mathrm{A}, 1_i, 1_s)$ for a 3-fold coincidence detection is calculated as follows. The probability to generate exactly one pair at Bob (please recall that the underlying distribution is thermal) is μ_SPDC, and that of generating one photon (with Poissonian distribution) at Alice is $\mu_\mathrm{A} e^{-\mu_\mathrm{A}}$. Hence, the probability to have one photon at the BS from both Alice and Bob is $\mu_{\mathrm{A}} t_{\mathrm{A}} e^{-\mu_{\mathrm{A}} t_{\mathrm{A}}} \mu_{\mathrm{SPDC}} t_{\mathrm{i}}$, where t_{A} is the transmission probability from Alice to Charlie and t_{i} is the transmission probability from Bob to Charlie. Since the probability for these photons to be projected onto $|\Psi^-\rangle_{\mathrm{Ai}}$ is 1/4, we get

$$P(1_{\mathrm{A}}, 1_{\mathrm{i}}, 1_{\mathrm{s}}) = \frac{1}{4} \mu_{\mathrm{SPDC}} \mu_{\mathrm{A}} t_{\mathrm{A}} e^{-\mu_{\mathrm{A}} t_{\mathrm{A}}} t_{\mathrm{i}} t_{\mathrm{s}} \eta_{\mathrm{BSM}}^2 \eta_{\mathrm{s}}, \tag{D.10}$$

where η_{BSM} is the efficiency of the detectors used for the BSM, η_{s} is the efficiency of the detectors used for the signal photons, and t_{s} is the transmission of the signal photons. Refer to Supplementary Figure D.6.

Following a similar procedure we find

$$\begin{aligned} P(0_{\mathrm{A}}, 2_{\mathrm{i}}, 2_{\mathrm{s}}) &= \frac{1}{4} \mu_{\mathrm{SPDC}}^2 e^{-\mu_{\mathrm{A}} t_{\mathrm{A}}} t_{\mathrm{i}}^2 \eta_{\mathrm{BSM}}^2 (1 - (1 - t_{\mathrm{s}} \eta_{\mathrm{s}})^2), \\ P(2_{\mathrm{A}}, 0_{\mathrm{i}}, 1_{\mathrm{s}}) &= \frac{1}{4} \mu_{\mathrm{SPDC}} (\mu_{\mathrm{A}} t_{\mathrm{A}})^2 \frac{e^{-\mu_{\mathrm{A}} t_{\mathrm{A}}}}{2} (1 - t_{\mathrm{i}}) \eta_{\mathrm{BSM}}^2 t_{\mathrm{s}} \eta_{\mathrm{s}}, \\ P(1_{\mathrm{A}}, 1_{\mathrm{i}}, 2_{\mathrm{s}}) &= \frac{1}{2} \mu_{\mathrm{SPDC}}^2 (\mu_{\mathrm{A}} t_{\mathrm{A}}) e^{-\mu_{\mathrm{A}} t_{\mathrm{A}}} (1 - t_{\mathrm{i}}) t_{\mathrm{i}} \eta_{\mathrm{BSM}}^2 (1 - (1 - t_{\mathrm{s}} \eta_{\mathrm{s}})^2). \end{aligned} \tag{D.11}$$

If the photons at the BS are partially indistinguishable and assuming input states are prepared as equal superpositions of $|e\rangle$ and $|l\rangle$, e.g. $|+\rangle$, the teleported state will correspond to the desired state with probability $\mathcal{V}$, and with probability $(1 - \mathcal{V})$, it will correspond to a completely mixed state ($\mathcal{V}$ is the degree of indistinguishability). From Eq. (D.9), the teleportation fidelity of these input states is given by

$$F_{+/-} = \frac{1}{2} + \frac{\mathcal{V}[P(1_{\mathrm{A}}, 1_{\mathrm{i}}, 1_{\mathrm{s}}) + P(1_{\mathrm{A}}, 1_{\mathrm{i}}, 2_{\mathrm{s}})]}{2[P(1_{\mathrm{A}}, 1_{\mathrm{i}}, 1_{\mathrm{s}}) + P(1_{\mathrm{A}}, 1_{\mathrm{i}}, 2_{\mathrm{s}}) + P(0_{\mathrm{A}}, 2_{\mathrm{i}}, 2_{\mathrm{s}}) + P(2_{\mathrm{A}}, 0_{\mathrm{i}}, 1_{\mathrm{s}})]}. \tag{D.12}$$

Likewise, we can also estimate the fidelity for the teleportation of $|e\rangle$ or $|\ell\rangle$. Note that for these states, multiphoton contributions from Alice will not result in any $|\Psi^-\rangle_{\mathrm{Ai}}$ BSM detection. Also, the degree of indistinguishability, $\mathcal{V}$, has no effect since HOM interference

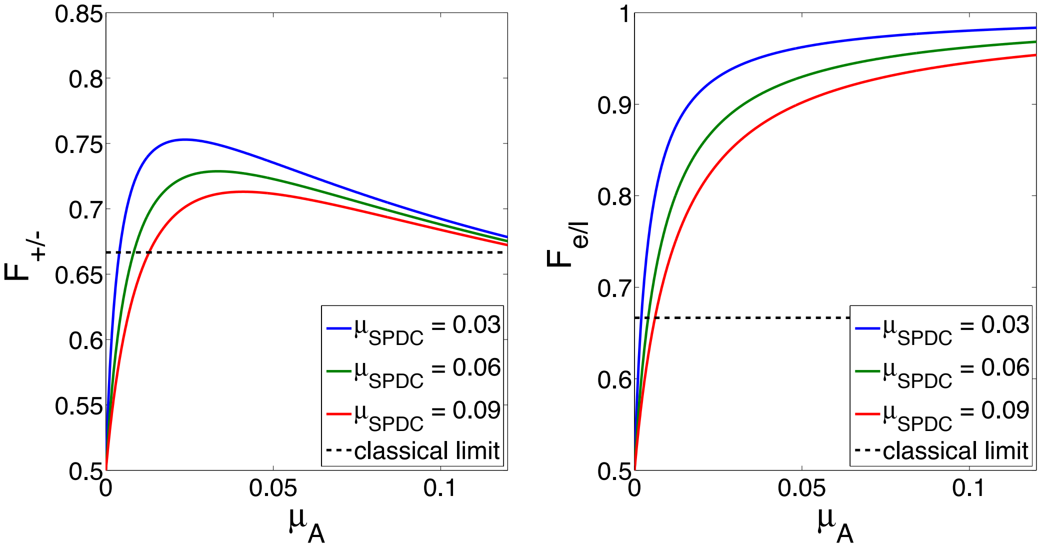


Figure D.12: Fidelities for different μ_{SPDC} as a function of μ_{A}. The curves with $\mu_{\text{SPDC}} = 0.06$ correspond to our experimental conditions. **Left:** Fidelity for equal-superposition states $F_{+/-}$. Notice that, by lowering μ_{SPDC}, the maximum fidelity increases due to reduced contribution of multiphoton events. **Right:** Fidelity for early or late states $F_{e/l}$. Notice that, by decreasing μ_{SPDC}, the fidelity increases due to the reduction of multiphoton events stemming from the SPDC source. For a given μ_{SPDC}, the fidelity keeps increasing with μ_{A} since multiphoton events from Alice do not result in any BSM.

is not required to faithfully complete the protocol in this basis. Thus, the fidelity is

$$F_{e/l} = \frac{P(1_{\text{A}}, 1_{\text{i}}, 1_{\text{s}}) + P(1_{\text{A}}, 1_{\text{i}}, 2_{\text{s}}) + 0.5P(0_{\text{A}}, 2_{\text{i}}, 2_{\text{s}})}{P(1_{\text{A}}, 1_{\text{i}}, 1_{\text{s}}) + P(1_{\text{A}}, 1_{\text{i}}, 2_{\text{s}}) + P(0_{\text{A}}, 2_{\text{i}}, 2_{\text{s}})}. \tag{D.13}$$

Supplementary Figure D.12 shows fidelities predicted by our model as a function of μ_{A}, for $\mu_{\text{SPDC}} = [0.03; 0.06; 0.09]$. The transmission probabilities, detector efficiencies and the degree of indistinguishability were chosen according to our experimental conditions: $t_{\text{i}} = 0.015$, $t_{\text{s}} = 0.01$, $t_{\text{A}} = 0.24$, $\eta_{\text{BSM}} = 0.7$, $\eta_{\text{s}} = 0.65$, and $\mathcal{V} = 0.68$. The fidelities are plotted for values of μ_{A} between 0 and 0.12. As μ_{A} increases, we see a steady increase in the fidelity, reaching a maximum when the probabilities for the BS input receiving exactly one photon from Alice and exactly one from Bob are equal [47]. For larger values of μ_{A},

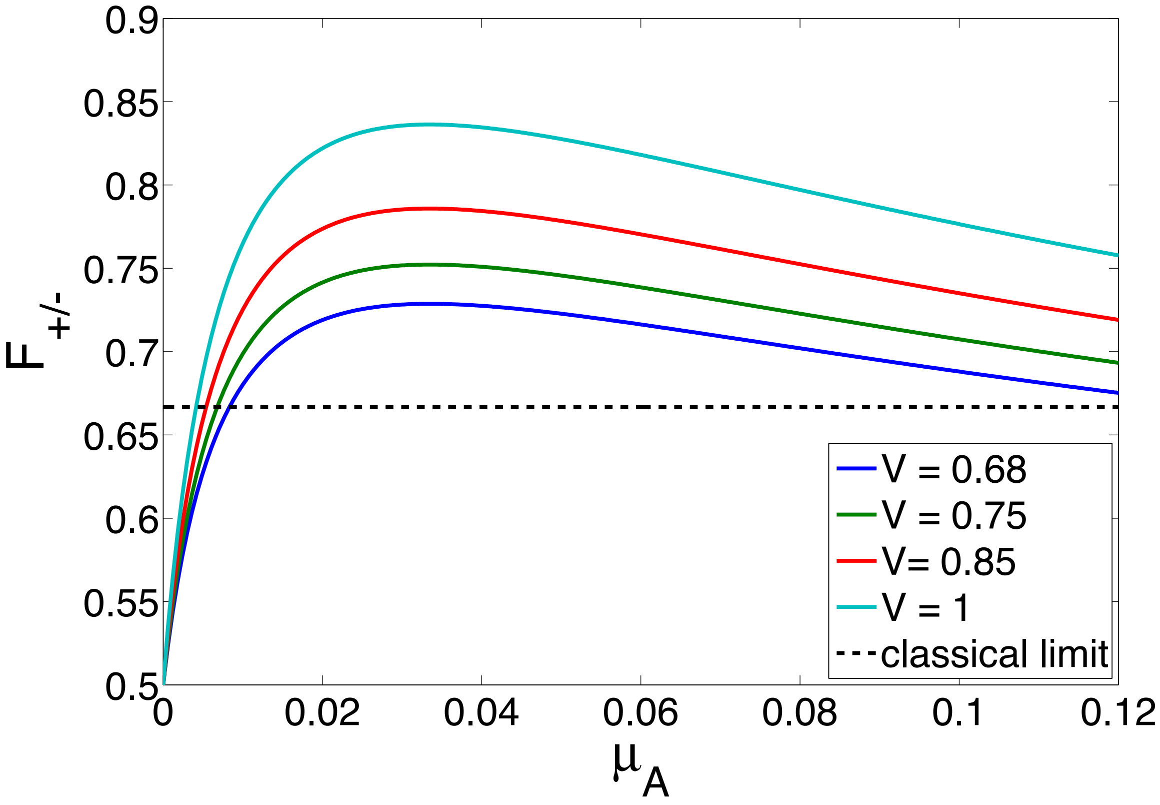


Figure D.13: Fidelity $F_{+/-}$ for different degrees of indistinguishability $\mathcal{V}$ as a function of μ_{A}. Note that the maximum fidelity increases as the indistinguishability of photons, $\mathcal{V}$ increases.

the contribution of multiphoton events increases, thus reducing the fidelity. Conversely, we find higher fidelities for smaller values of μ_{SPDC}. For $|e\rangle$ and $|\ell\rangle$, the fidelity increases as we increase μ_{A}.

Since we found in Supplementary Section D that the indistinguishability is not perfect in our experimental setup, in Supplementary Figure D.13, we plot $F_{+/-}$ as a function of μ_{A} for different values of $\mathcal{V}$. We set $\mu_{\mathrm{SPDC}} = 0.06$, and the rest of the parameters were chosen as in Supplementary Figure D.12. As expected, we observe that better fidelities are obtained as $\mathcal{V}$ increases. The maximum fidelity attainable is 0.835 for $\mathcal{V} = 1$. This provides an upper limit of the fidelity $F_{+/-}$ that we can obtain in our experiment.

Bounding the teleportation fidelity of single photon using decoy state method

The decoy state method was originally developed to overcome the photon number splitting attack in quantum key distribution — it allows estimating the amount of key obtained from states containing one, and only one, photon [48, 49]. We recently expanded the decoy state method to verify the quantum nature of a memory [37], and here we use it for the first time to demonstrate the quantum nature of teleportation in our experiment [49]. This requires the average fidelity over a certain set of input states to exceed 2/3, provided these states are encoded into individual photons.

First, we define the error rate

$$E_\phi = \frac{C_{|\phi_\perp\rangle\langle\phi_\perp|}}{C_{|\phi_\perp\rangle\langle\phi_\perp|} + C_{|\phi\rangle\langle\phi|}}, \tag{D.14}$$

where, $C_{|\phi_\perp\rangle\langle\phi_\perp|}$ denotes the number of measured events corresponding to the state $|\phi_\perp\rangle$, while the expected teleported state is $|\phi\rangle$. Since $|\phi_\perp\rangle$ corresponds to a state orthogonal to $|\phi\rangle$, a count of this type constitutes an error. Comparing with the expression for the fidelity of the quantum teleportation in Eq. (D.9), we find the simple relation $F_\phi = 1 - E_\phi$. The decoy state method allows us to estimate the impact of a quantum channel on qubits encoded onto single photons. In the method, Alice creates phase-randomized attenuated laser pulses and randomly modulates between different intensities for each pulse, known as signal and decoy states. The individual measurement statistics collected for different intensities goes into an estimate of the lower bound of the count rates, and an upper bound on the errors, that would have resulted from single-photon emissions from Alice. Based on Eq. (25) from Ref. [[49]], the error rate $E^{(1)}$ for the single photon component in a coherent pulses is upper bounded by $E_{\mathrm{U}}^{(1)}$, which is

$$E^{(1)} \leq E_{\mathrm{U}}^{(1)} = \frac{E^{(\mu_{\mathrm{d}})} Q^{(\mu_{\mathrm{d}})} e^{\mu_{\mathrm{d}}} - E^{(0)} Y^{(0)}}{\mu_{\mathrm{d}} Y_{\mathrm{L}}^{(1)}}. \tag{D.15}$$

Here, $\mu_{\rm d}$ is the mean photon number per qubit encoded into a decoy state; $Q^{(\mu_{\rm d})}$ is the corresponding gain (i.e. the probability for a 3-fold coincidence when creating pulses with mean photon number $\mu_{\rm d}$ at Alice's), and $E^{(\mu_{\rm d})}$ is the corresponding error rate; $E^{(0)}$ is the error rate for a zero-photon (vacuum) input at Alice's; $Y^{(0)}$ and $Y_{\rm L}^{(1)}$ are the yield for a zero-photon input and the lower bound for the yield of a single photon input, respectively. The values $Q^{(\mu_{\rm d})}$, $E^{(\mu_{\rm d})}$, $Y^{(0)}$ and $E^{(0)}$ can be measured directly in the experiment.

Given a phase randomized coherent state with a mean photon number of μ, the gain can be expressed as

$$Q^{(\mu)} = \sum_{n=0}^{\infty} \frac{Y^{(n)} \mu^n e^{-\mu}}{n!}, \tag{D.16}$$

where the yield of an n-photon state, $Y^{(n)}$, is the conditional probability of a detection given that an n-photon state was sent from Alice. These yields, with an exception of the yield of the vacuum state $Y^{(0)}$, can generally not be measured directly. Fortunately, one can derive a lower bound $Y_{\rm L}^{(1)}$ for the single photon yield (applied in Eq. D.15), which is discussed in Ref. [8]:

$$Y^{(1)} \geq Y_{\rm L}^{(1)} = \frac{\mu_{\rm s}}{\mu_{\rm s}\mu_{\rm d} - \mu_{\rm d}^2} (Q^{(\mu_{\rm d})} e^{\mu_{\rm d}} \tag{D.17}$$

$$-\frac{\mu_{\rm d}^2}{\mu_{\rm s}^2} Q^{(\mu_{\rm s})} e^{\mu_{\rm s}} - \frac{\mu_{\rm s}^2 - \mu_{\rm d}^2}{\mu_{\rm s}^2} Y^{(0)}), \tag{D.18}$$

where $\mu_{\rm s} > \mu_{\rm d}$ is the mean photon number of the signal state. $Q^{(\mu_{\rm s})}$ is the corresponding gain of the signal state; it is also measurable. Thus, we can calculate an upper bound of the error rate $E_U^{(1)}$ from Eqs. (D.15) and (D.17). In turn, this allows computing a lower bound on the fidelity in the quantum teleportation experiment:

$$F^{(1)} = 1 - E^{(1)} \geq 1 - E_{\rm U}^{(1)} \equiv F_{\rm L}^{(1)}. \tag{D.19}$$

In our experiment, the quantum channel, whose effect on single photons emitted at Alice's we want to characterize, is given by the concatenation of direct qubit transmission from Alice to Charlie, and teleportation from Charlie to Bob. To implement the decoy state method, Alice prepares qubits with three different mean photon numbers (μ_s, μ_d and vaccuum) and sends them to Charlie. This allows us to obtain a bound on the fidelity of the teleportation experiment that we would obtained had we utilized true single photons to encode qubits.

We also use our theoretical model to predict the results of the decoy state protocol. We express Q^μ and $E^\mu_{1/0}$ using the variables in our model as

$$Q^\mu = P(1_\mathrm{A}, 1_\mathrm{i}, 1_\mathrm{s}) + P(0_\mathrm{A}, 2_\mathrm{i}, 2_\mathrm{s}) + P(2_\mathrm{A}, 0_\mathrm{i}, 1_\mathrm{s}) + P(1_\mathrm{A}, 1_\mathrm{i}, 2_\mathrm{s}) \tag{D.20}$$

$$E^\mu_{+/-\ (e/l)} = 1 - F_{+/-\ (e/l)}. \tag{D.21}$$

We calculate the lower bound of $F^{(1)}_{+/-}$, and $F^{(1)}_{e/l}$ using Eqs. (D.15), (D.17) and (D.20). Finally, we obtain $F^{(1)}_\mathrm{avg} = 2/3\ F^{(1)}_{+/-} + 1/3\ F^{(1)}_{e/l}$, with different μ_d and μ_s, as shown in Supplementary Figure D.14. Two different areas are shown, the white area corresponds to the fidelities that can be reached by classical strategies. The coloured area (not grey) corresponds to fidelities that can not be obtained classically. Note that $F^{(1)}_\mathrm{avg}$ depends mostly on μ_d. $F^{(1)}_\mathrm{avg}$ increases as μ_d decreases, since the decoy method can bound the contribution of higher multiphoton events more tightly.

With the help of this model, we set μ_s and μ_d in our experiment to be 0.028 and 0.014, respectively. With these values, we can exceed the classical bound of 2/3 for the single photon fidelity significantly, as shown in Supplementary Figure D.14. Moreover, these values of μ_s and μ_d result in rates for 3-fold coincidence counts of several per minute (see Supplementary section D). Also, this choice leads to a HOM visibility (see Supplementary Figure D.10) that is sufficiently large to allow for the timing feedback (see Methods in

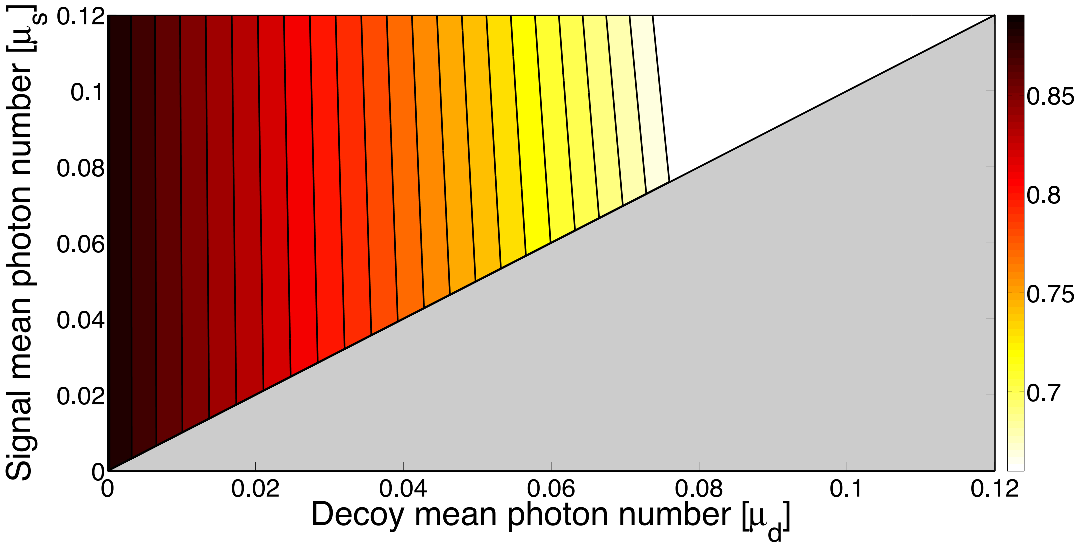


Figure D.14: Predicted average single photon fidelity $F^{(1)}_{\text{avg}}$ as a function of μ_{d} and μ_{s}. Fidelities are indicated using the colour gradient shown on the right. The region in white corresponds to $F^{(1)}_{\text{avg}} < 2/3$, which can be achieved using classical strategies. The grey area corresponds to ($\mu_{\text{d}} > \mu_{\text{s}}$), which is not covered by decoy state method.

the main text).

Experimental data and model comparison

In this section, we present the experimental data that is used to calculate fidelities using the decoy state method.

Decoy state method

Table D.1 and D.2 shows measured gains and fidelities for different mean photon numbers ($\mu_{\text{s}} = 0.028$ and $\mu_{\text{d}} = 0.014$).

Table D.1: Gains [Hz] for different input states and signal and decoy mean photon numbers.

state	signal	decoy	vacuum
$\lvert+\rangle$	0.35 ± 0.01	0.18 ± 0.01	0.038 ± 0.003
$\lvert+i\rangle$	0.35 ± 0.02	0.18 ± 0.01	0.038 ± 0.003
$\lvert e\rangle$	0.14 ± 0.01	0.09 ± 0.01	0.016 ± 0.002
$\lvert\ell\rangle$	0.14 ± 0.01	0.08 ± 0.01	0.016 ± 0.002

Table D.2: Fidelities for different mean photon number and states.

state	signal	decoy	vacuum
$\lvert+\rangle$	0.70 ± 0.02	0.72 ± 0.02	0.50 ± 0.05
$\lvert+i\rangle$	0.70 ± 0.02	0.73 ± 0.02	0.50 ± 0.05
$\lvert e\rangle$	0.91 ± 0.01	0.87 ± 0.02	0.63 ± 0.07
$\lvert\ell\rangle$	0.89 ± 0.02	0.88 ± 0.03	0.63 ± 0.07

Comparison of measured and predicted fidelities

Table D.3 compares experimentally obtained and predicted fidelities (from our model) for the two mean photon numbers ($\mu_{\mathrm{s}} = 0.028$ and $\mu_{\mathrm{d}} = 0.014$) that were chosen in the decoy state method per qubit emitted at Alice's. Table D.4 compares experimentally observed fidelities, derived after quantum state tomography of different input states, with predicted fidelities from our model. The experimental values are in good agreement with the expected fidelities.

Table D.3: Comparison of fidelities obtained experimentally using the decoy values with predicted values for $\mu_{\mathrm{SPDC}} = 0.06$.

	experiment		model	
	μ_s	μ_d	μ_s	μ_d
$\lvert+\rangle$	0.70 ± 0.02	0.72 ± 0.02	0.73	0.70
$\lvert+i\rangle$	0.70 ± 0.02	0.73 ± 0.02	0.73	0.70
$\lvert e\rangle$	0.91 ± 0.01	0.87 ± 0.02	0.89	0.82
$\lvert l\rangle$	0.89 ± 0.02	0.88 ± 0.03	0.89	0.82

Table D.4: Comparison of fidelities obtained after quantum state tomography with predicted values for $\mu_{SPDC} = 0.045$ and $\mu_c = 0.014$.

	experiment	model
$\lvert + \rangle$	0.75 ± 0.03	0.72
$\lvert +i \rangle$	0.71 ± 0.03	0.72
$\lvert e \rangle$	0.86 ± 0.03	0.85
$\lvert l \rangle$	0.89 ± 0.03	0.85

Bibliography

[1] Bennett, C. H. *et al.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895-1899 (1993).

[2] Pirandola, S. Eisert, J. Weedbrook, C. Furusawa, A. & Braunstein, S. L. Advances in quantum teleportation. *Nat. Phot.* **9**, 641-652 (2015)

[3] Landry, O. van Houwelingen, J. A. W. Beveratos, A. Zbinden, H. & Gisin, N. Quantum teleportation over the Swisscom telecommunication network. *JOSA B* **24**, 398-403 (2007).

[4] Hensen, B. *et al.*, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **526**, 682-686 (2015).

[5] Sangouard, N. Simon, C. De Riedmatten, H. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. of Mod. Phys.* **83**, 33-80 (2011).

[6] Kimble, H. J. The quantum Internet. *Nature* **453**, 1023-1030 (2008).

[7] Yin, J. *et al.* Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. *Nature* **488**, 185-188 (2012).

[8] Ma, X-S. *et al.* Quantum teleportation over 143 kilometres using active feed-forward. *Nature* **489**, 269-273 (2012).

[9] Lvovsky, A. I. Sanders, B. C. & Tittel, W. Optical quantum memory. *Nat. Phot.* **3**, 706-714 (2009).

[10] Żukowski, M. Zeilinger, A. Horne, M. A. & Ekert, A. K. “Event-ready-detectors” Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **71**, 4287-4290 (1993).

[11] Rubenok, A. Slater, J. A. Chan, P. Lucio-Martinez, I. & Tittel, W. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111**, 130501 (2013).

[12] Marcikic, I. De Riedmatten, H. Tittel, W. Zbinden, H. & Gisin, N. Long-distance teleportation of qubits at telecommunication wavelengths. *Nature* **421**, 509-513 (2003).

[13] de Riedmatten, H. *et al.* Long distance quantum teleportation in a quantum relay configuration. *Phys. Rev. Lett.* **92**, 047904 (2004).

[14] Bussières, F. *et al.* Quantum teleportation from a telecom-wavelength photon to a solid-state quantum memory. *Nat. Phot.* **8**, 775-778 (2014).

[15] Takesue, H. *et al.* Quantum teleportation over 100 km of fiber using highly efficient superconducting nanowire single-photon detectors. *Optica* **2**, 832-835 (2015).

[16] Ma, X. S. *et al.* Experimental delayed-choice entanglement swapping. *Nat. Phys.* **8**, 479-484 (2012).

[17] Megidish, E. *et al.* Entanglement swapping between photons that have never coexisted. *Phys. Rev. Lett.* **110**, 210403 (2013).

[18] Massar, S. & Popescu, S. Optimal extraction of information from finite quantum ensembles. *Phys. Rev. Lett.* **74**, 1259–1263 (1995).

[19] Lo, H-K. Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).

[20] Wang, X. B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).

[21] Brendel, J. Gisin, N. Tittel, W. & Zbinden, H. Pulsed energy-time entangled twin-photon source for quantum communication. *Phys. Rev. Lett.* **82**, 2594-2597 (1999).

[22] Marsili, F. *et al.* Detecting single infrared photons with 93 % system efficiency. *Nat. Phot.* **7**, 210-214 (2013).

[23] Sinclair, N. *et al.* Spectral multiplexing for scalable quantum photonics using an atomic frequency comb quantum memory and feed-forward control. *Phys. Rev. Lett.* **113**, 053603 (2014).

[24] Hong, C. K. Ou, Z. Y. & Mandel, L. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 2044-2046 (1987).

[25] Krovi, H. *et al.* W. Practical quantum repeaters with parametric down-conversion sources. *Applied Physics B* **122**, 52 (2016).

[26] Thiel, C. W. Sinclair, N. Tittel, W. & Cone, R. L. Optical decoherence studies of $\mathrm{Tm}^{3+} : \mathrm{Y}_3\mathrm{Ga}_5\mathrm{O}_{12}$. *Phys. Rev. B* **90**, 214301 (2014).

[27] Valivarthi, R. *et al.* Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors. *Opt. Expr.* **22**, 24497-24506 (2014).

[28] http://www.wavelengthreferences.com/pdf/Data

[29] Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Physical review letters* **108**, 130502 (2012).

[30] Sun, Q.-C. *et al.* Quantum teleportation with independent sources over an optical fibre network. *arXiv* **1602.07081**, (2016).

[31] Bennett, C. H. Brassard, G. Crépeau, C. Jozsa, R. Peres, A. and Wootters, W. K. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895-1899 (1993).

[32] Salart, D. et al. Testing the speed of 'spooky action at a distance'. *Nature* **454**, 861 (2008).

[33] Yin, J. et al. Lower bound on the speed of nonlocal correlations without locality and measurement choice loopholes. *Phys. Rev. Lett.* **110**, 260407 (2013).

[34] Yin, J. et al. Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. *Nature* **488**, 185188 (2012).

[35] Ma, X.S. et al. Quantum teleportation over 143 kilometres using active feed-forward. *Nature* **489**, 269273 (2012).

[36] Sangouard, N. et al. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **83**, 33 (2011).

[37] Sinclair, N. et al. Spectral Multiplexing for Scalable Quantum Photonics using an Atomic Frequency Comb Quantum Memory and Feed-Forward Control. *Phys. Rev. Lett.* **113**, 053603 (2014).

[38] Sun, Q.C. et al. Quantum teleportation with independent sources over an optical fibre network. *arXiv* **1602.07081** (2016).

[39] Bussières, F. et al. Quantum teleportation from a telecom-wavelength photon to a solid-state quantum memory. *Nat. Phot.* **8**, 775 (2014).

[40] Takesue, H. et al. Quantum teleportation over 100 km of fiber using highly efficient superconducting nanowire single-photon detectors. *Optica* **2**, 832-835 (2015).

[41] Marcikic, I., de Riedmatten, H. Tittel, W. Zbinden, H. and Gisin N. Long-distance teleportation of qubits at telecommunication wavelengths. *Nature* **421**, 509-513 (2003).

[42] de Riedmatten, H. *et al.* Long Distance Quantum Teleportation in a Quantum Relay Configuration. *Phys. Rev. Lett.* **92**, 047904 (2004).

[43] Landry, O. et al. Quantum teleportation over the Swisscom telecommunication network. *J. Opt. Soc. Am. B* **24**, 2 (2007).

[44] Hensen, B. et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **526**, 682-686 (2015).

[45] Hong, C. K. Ou, Z. Y. and Mandel, L. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 2044-2046 (1987).

[46] de Riedmatten, H. Marcikic, I. Tittel, W. Zbinden, H. and Gisin, N. Quantum interference with photon pairs created in spatially separated sources. *Phys. Rev. A.* **67**, 022301 (2003).

[47] Rarity, J. G. Tapster, P. R. and Loudon, R. Non-classical interference between independent sources. *arXiv* preprint quant-ph/9702032 (1997).

[48] Lo, H-K. Ma, X. Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).

[49] Ma, X. Qi, B. Zhao, Y. and Lo, H-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).

[50] Massar, S. and Popescu, S. Optimal Extraction of Information from Finite Quantum Ensembles. *Phys. Rev. Lett.* **74**, 1259-1263 (1995).

Appendix E

Paper V

Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors

Optics express 22.20 (2014): 24497-24506.

R. Valivarthi[1,2], I. Lucio-Martinez[1,2], A. Rubenok[1,2,†], P. Chan[1,3], F. Marsili[5], V. B. Verma[4], M. D. Shaw[5], J. A. Stern[5], J. A. Slater[1,2], D. Oblak[1,2], S. W. Nam[4], W. Tittel[1,2]

1. Institute for Quantum Science and Technology, University of Calgary, Calgary, AB, T2N 1N4, Canada

2. Department of Physics and Astronomy, University of Calgary, Calgary, AB, T2N 1N4, Canada

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

4. National Institute of Standards and Technology, Boulder, CO, 80305, USA

5. Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, 91109, USA

Abstract

We experimentally demonstrate a high-efficiency Bell state measurement for time-bin qubits that employs two superconducting nanowire single-photon detectors with short

dead-times, allowing projections onto two Bell states, $|\psi^-\rangle$ and $|\psi^+\rangle$. Compared to previous implementations for time-bin qubits, this yields an increase in the efficiency of Bell state analysis by a factor of thirty.

Bibliography

[1] N. Sangouard, C. Simon, H. de Riedmatten and N. Gisin,“Quantum repeaters based on atomic ensembles and linear optics,” Rev. Mod. Phys, **83**, 33 (2011).

[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels,” Phys. Rev. Lett., **70**, 1895 (1993).

[3] K. Mattle, H. Weinfurter, P. G. Kwiat and A. Zeilinger, “Dense Coding in Experimental Quantum Communication,” Phys. Rev. Lett., **76**, 4656 (1996).

[4] H.-K. Lo, M. Curty and B. Qi, “Measurement-device-independent quantum key disitrbution,” Phys. Rev. Lett., **108**, 130503 (2012).

[5] N. Lütkenhaus, J. Calsamiglia and K.-A. Suominen, “Bell measurements for teleportation,” Phys. Rev. A, **59**, 3295 (1999).

[6] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, “”Plug and play” systems for quantum cryptography,” Applied Physics Letters **70**, 793 (1997).

[7] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, “Pulsed energy-time enangled twin-photon source for quantum communication,” Phys. Rev. Lett. **82**, 2594 (1999).

[8] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, “Quantum cryptography using entangled photons in energy-time Bell states,” Phys. Rev. Lett. **84**, 4737 (2000).

[9] I. Marcikic, H. De Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, “Long-distance teleportation of qubits at telecommunication wavelengths,” Nature **421**, 509 (2003).

[10] H. De Riedmatten, I. Marcikic, J. A. W. van Houwelingen, W. Tittel, . Zbinden, N. Gisin, “Long-distance entanglement swapping with photons from separated sources,” Phys. Rev. A **71**, 050302 (2005).

[11] J. Jin, J. A. Slater, E. Saglamyurek, NJ. Sinclair, M. George, R. Ricken, D. Oblak, W. Sohler, and W. Tittel, “Two-photon interference of weak coherent laser pulses recalled from separate solid-state quantum memories,” Nature Comm. **4**, 2386 (2013).

[12] 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,” Phys. Rev. Lett., **111**, 130501 (2013).

[13] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang and J.-W. Pan, “Experimental Measurement-Device-Independent Quantum Key Distribution,” Phys. Rev. Lett., **111**, 130502 (2013).

[14] A. R. Dixon and J. F. Dynes and Z. L. Yuan and A. W. Sharpe and A. J. Bennet and A. J. Shields, “Ultrashort dead time of photon-counting InGaAs avalanche photodiodes,” Appl. Phys. Lett., **94**, 231113 (2009).

[15] J. Zhang, R. Thew, C. Barreiro and H. Zbinden, “Practical fast gate rate InGaAs/InP single-photon avalanche photodiodes,” Appl. Phys. Lett., **95**, 091103 (2009).

[16] J. Zhang, R. Thew, J.-D. Gautier, N. Gisin, H. Zbinden, “Comprehensive Characterization of InGaAs/InP Avalanche Photodiodes at 1550nm with an Active Quenching ASIC,” J. Quantum Electron., **45**, 792 (2009).

[17] J. A. W. van Houwelingen, N. Brunner, A. Beveratos, H. Zbinden, and N. Gisin,

"Quantum Teleportation with a Three-Bell-State Analyzer," Phys. Rev. Lett. **96**, 130502 (2006).

[18] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, " Superconducting nanowire single-photon detectors: physics and applications," Supercond. Sci. Technol., **25**, 063001 (2012).

[19] A. J. Kerman, E. A. Dauler, W. E. Keicher, J. K. W. Yang, K. K. Berggren, G. Goltsman and B. Voronov, "Kinetic-inductance-limited reset time of superconducting nanowire photon counters," Appl. Phys. Lett., **88**, 111116 (2006).

[20] B. S. Robinson, A. J. Kerman, E. A. Dauler, R. J. Barron, D. O. Caplan, M. L. Stevens, J. J. Carney, S. A. Hamilton, J. K. Yang, and K. K. Berggren,"781-Mbit/s photon-counting optical communications using a super-conducting nanowire detector," Opt. Lett., **31**, 444 (2006).

[21] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin and S. W. Nam, "Detecting single infrared photons with 93% system efficiency," Nat. Photon., **7**, 210-214 (2013).

[22] V. B. Verma, F. Marsili, S. Harrington, A. E. Lita, R. P. Mirin, and S. W. Nam, "A three-dimensional, polarization-insensitive superconducting nanowire avalanche photodetector," Appl. Phys. Lett., **101**, 251114 (2012).

[23] J. K. W. Yang, A. J. Kerman, E. A. Dauler, V. Anant, K. M. Rosfjord and K. K. Berggren, "Modeling the Electrical and Thermal Response of Superconducting Nanowire Single-Photon Detectors," IEEE Trans. on Appl. Supercond., **17**, 581(2007).

[24] X.-B. Wang, "Three-intensity decoy state method for device independent quantum key distribution with basis dependent errors," Phys. Rev. A, **87**, 012320 (2013).

[25] V. B. Verma, R. Horansky, F. Marsili, J. A. Stern, M. D. Shaw, A. E. Lita, R. P. Mirin, S. W. Nam, ”A four-pixel single-photon pulse-position array fabricated from WSi superconducting nanowire single-photon detectors,” Appl. Phys. Lett., **104**, 051115 (2014)

E.1 Introduction

Bell state measurements (BSMs) play a key role in linear optics quantum computation and many quantum communication protocols, e.g. quantum repeaters [1], quantum teleportation [2], dense coding [3] and some quantum key distribution protocols [4]. A complete BSM allows projecting any two-photon state deterministically and unambiguously onto the set of four maximally-entangled Bell states, i.e.

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$

and

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).$$

Unfortunately, it has been shown that a complete BSM is impossible when using linear optics and no auxiliary photons: the probability for a BSM to succeed (henceforward referred to as efficiency, η_{BSM}) in the case of two photons in completely mixed input states (e.g. two photons that are members of different entangled pairs) is, in principle, limited to 50% [5]. The standard approach to Bell state analysis uses a 50/50 beam splitter followed by single-photon detectors that allow (possibly using additional external optical elements) discriminating between orthogonal qubit states $|0\rangle$ and $|1\rangle$ (see figure E.1). This approach allows one to unambiguously project onto $|\psi^-\rangle$ and $|\psi^+\rangle$.

For instance, when implementing a BSM for polarization qubits, a projection onto $|\psi^-\rangle$ occurs if the two photons exit the beam splitter through two different ports and

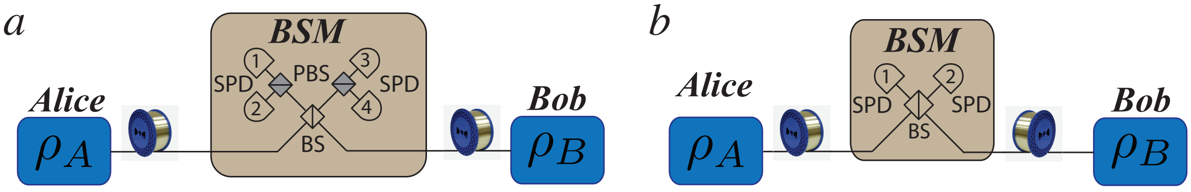


Figure E.1: Experimental setup used to perform BSMs for a) polarization qubits and b) time-bin qubits. Density matrices ρ_A and ρ_B characterize the states of the photons emitted at Alice's and Bob's, respectively. Optical components: beam splitter (BS) and single photon detectors (SPD).

are detected in orthogonal polarizations, leading to detections in detectors 1 and 4, or detectors 2 and 3 (for an illustration see Fig. E.1a). Furthermore, projections onto $|\psi^+\rangle$ happen if the two photons exit the beam splitter through the same port and, as before, are detected in orthogonal polarization states. This leads to detections in detectors 1 and 2, or detectors 3 and 4 (see Fig. E.1a). Other coincidence detections correspond to projections onto product states $|H\rangle|H\rangle \equiv |0\rangle|0\rangle$ and $|V\rangle|V\rangle \equiv |1\rangle|1\rangle$. Hence, this scheme allows achieving the maximum efficiency value of 50% if one considers single photon detectors with unity detection efficiency. Assuming realistic detectors with efficiency η_{det}, the BSM efficiency is reduced to

$$\eta_{BSM} = \frac{1}{2}\eta_{det}^2. \tag{E.1}$$

In addition to polarization, another widely used degree of freedom to encode qubits is time. In this case photons are generated in a superposition of two temporal modes $|early\rangle \equiv |0\rangle$ and $|late\rangle \equiv |1\rangle$ – so-called time-bin qubits. Time-bin qubits are particularly well suited for transmission over optical fiber (and thus generally encoded into photons at telecommunication wavelength), and have been used for a large number of experiments [6–8], including experiments that require projections onto Bell states [9–13]. BSMs with time-bin qubits generalize the scheme introduced above for polarization qubits but require only a single beam splitter as illustrated in Fig. E.1b. The temporal detection pattern of photons after passing the beam-splitter (see Fig. E.2a) corresponds to different bell-state projections. A projection onto the singlet $|\psi^-\rangle$ state occurs if one of the two detectors registers a photon in the early time bin and the second detector registers a photon in the late time bin (see Fig. E.2b). On the other hand, a projection onto $|\psi^+\rangle$ happens if a detector registers one photon in the early time bin, and the same detector detects the second photon in the late bin (see Fig. E.2c).

However, a problem arises if the detection of a photon is followed by dead-time during which the detector cannot detect a subsequent photon. For example, for commercial InGaAs-based single photon detectors (SPDs), which are widely used for quantum communication applications including BSM with time-bin qubits, this dead-time is typically around 10 μs[1]. This dead-time is necessary to suppress afterpulsing due to trapped carriers that are released after a detection and cause subsequent detection signals [16]. The dead-time of the detectors previously employed for the BSM have always been orders of magnitude longer than the maximally achievable time difference between early and late temporal modes, which is limited by the required frequency stability of the source laser for the time-bins. Thus, commercial InGaAs SPDs have usually restricted BSMs with time-bin qubits to projections onto $|\psi^-\rangle$, reducing the maximum efficiency of the BSM from 50% to 25%. The only exception is [17], where the unambiguous projections onto three Bell states with theoretically maximum probability of 5/16≈31% was proposed and a proof-of-principle demonstration reported. Taking a typical detection efficiency for InGaAs SPDs of 15% into account, the highest efficiency of a BSM for time-bin qubits is currently thus only around 1%. This includes the demonstrations reported in [13–15] and [17].

[1] To the best of our knowledge, the exceptions are [13], where frequency conversion and Si-APDs were employed, and [14,15], where InGaAs-based SPDs with dead-times of 2 ns and 10 ns and quantum detection efficiencies of ≈10% have been reported. However, none of the last-mentioned detectors have

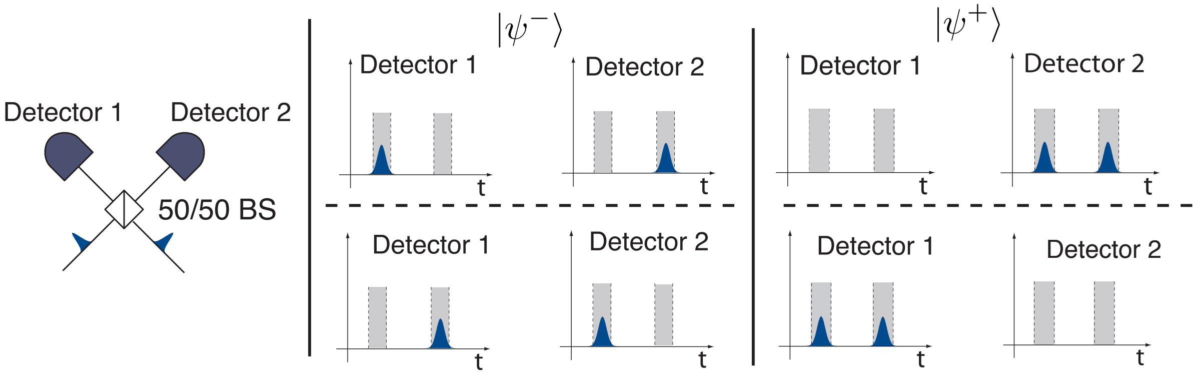


Figure E.2: a) General setup for Bell state measurement for time-bin qubits using linear optics and single photon detectors (SPD). b) Detection pattern for projections onto $|\psi^-\rangle$ and (c) $|\psi^+\rangle$.

In this paper we present an efficient BSM for time-bin qubits encoded into telecommunication photons with projections onto the $|\psi^-\rangle$ as well as the $|\psi^+\rangle$ Bell state. Towards this end, we employ two superconducting nanowire single photons detectors (SNSPDs), which, in addition to short dead-times, feature low dark count rates and system detection efficiencies of 76%. This leads to an increase of η_{BSM} by a factor of thirty compared to previous implementations, which is an important improvement in view of future applications of quantum information processing involving many BSMs, e.g. quantum repeaters.

The remainder of this article is structured as follows. In section E.2 we describe the single-photon detectors employed to perform the measurements, and in section E.3 we present the details of the experimental setup. The results of our measurements are presented and discussed in section E.4. Finally, in section E.5, we present our conclusions and outlook.

been used for BSMs with time-bin qubits.

E.2 Superconducting single photon detectors with short dead-times

Recent years have seen great progress in the development of single-photon detectors for telecommunication wavelengths. Arguably, the best detectors today are based on the transition of a superconducting nanowire into the resistive state [18], and many benchmark results have been reported with these SNSPDs. This includes dead-times as small as 10 ns [19,20], and quantum efficiencies up to 93% at 1550 nm [21]. Furthermore, unlike InGaAs SPDs, which require gating, SNSPDs are inherently free running, show no afterpulsing, and feature very low dark count rates on the Hz level [21].

We employ SNSPDs that have been developed and fabricated at the National Institute for Standards and Technology (NIST) and the Jet Propulsion Laboratory (JPL). The detectors are based on one, or two mutually orthogonal, tungsten silicide (WSi) nanowire meanders (we refer to the two different detectors as detector 1 and 2, respectively – see Fig E.3 a for a sketch of detector 2. The detector with two meanders features a detection efficiency that is highly insensitive to photon polarization [22], whereas the single meander version experiences up to 10% variation in efficiency at different polarizations. The two SNSPDs are mounted on an adiabatic diamagnetic refrigeration (ADR) stage inside a pulse-tube cooler, and are operated at a temperature around 800 mK. The setup for characterizing and operating the detectors is sketched in Fig. E.3a. The SNSPDs are represented by a kinetic inductance L_k and load resistance $R_l = 50\ \Omega + R_s$, where the first term on the right-hand-side is the impedance of the output coaxial cable and R_s is an additional and optional series resistor. A sample of the detection signal is shown in Fig. E.3b. The detector quantum efficiencies were measured at 1550 nm wavelength to be $77.5 \pm 0.7\%$ and $76.2 \pm 0.9\%$ for detectors 1 and 2, respectively.

To assess the detector dead-times, we illuminate the SNSPDs with weak continuous wave (cw) light and log the time Δt between subsequent detections, as illustrated in

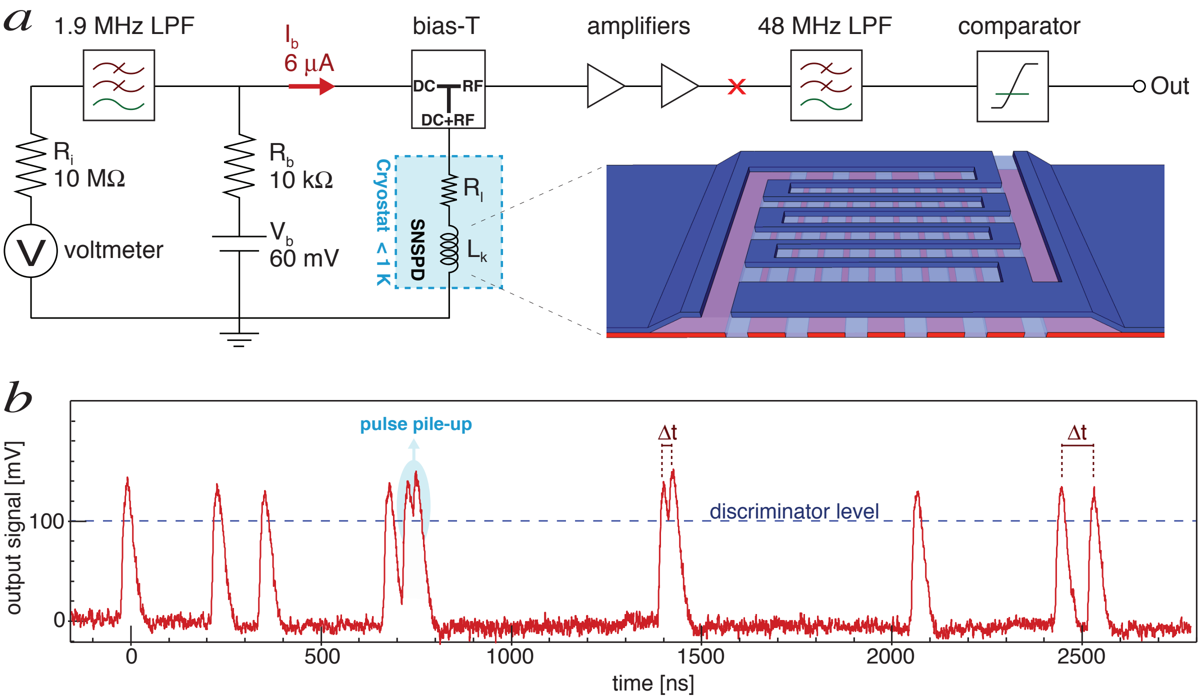


Figure E.3: Detector setup and signal. a) Electrical diagram of the SNSPD setup. The $R_b = 10$ kΩ bias resistor translates the 60 mV bias voltage into a $I_b = 6$ μA bias current, which is directed to the superconducting detectors via the DC-port of the bias-T. The RF-port of the bias-T directs the photon detection signal through two amplifiers and a low-pass-filter (LPF) to a comparator, which generates a TTL output signal. The parallel connected voltmeter measures the voltage drop over the SNSPD and allows verifying that it is in the superconducting state. The panel also shows a sketch of an SNSPD consisting of two meanders. b) Single photon detection signals of detector 2 immediately after the amplifiers (marked by an x in figure a). A few detection inter-arrival times Δt are indicated for illustration.

Fig. E.3b. Histograms of these inter-arrival detection times reveal the minimum time separation τ between detection events – during this time, the SNSPDs cannot detect another photon either because of the intrinsic time it takes the current to reflow or because of a pulse pile-up in which the signal does not cross the discriminator level between two consecutive incident photons and thus only the first detection event is registered. The measurements, with a 50 Ω coaxial cable attached to the detectors, shown in Fig. E.4 by the solid lines, gives a dead-time τ on the order of 30 ns for detector 1 and 100 ns for detector 2. This dissimilarity of dead-time is due to the difference in kinetic inductance

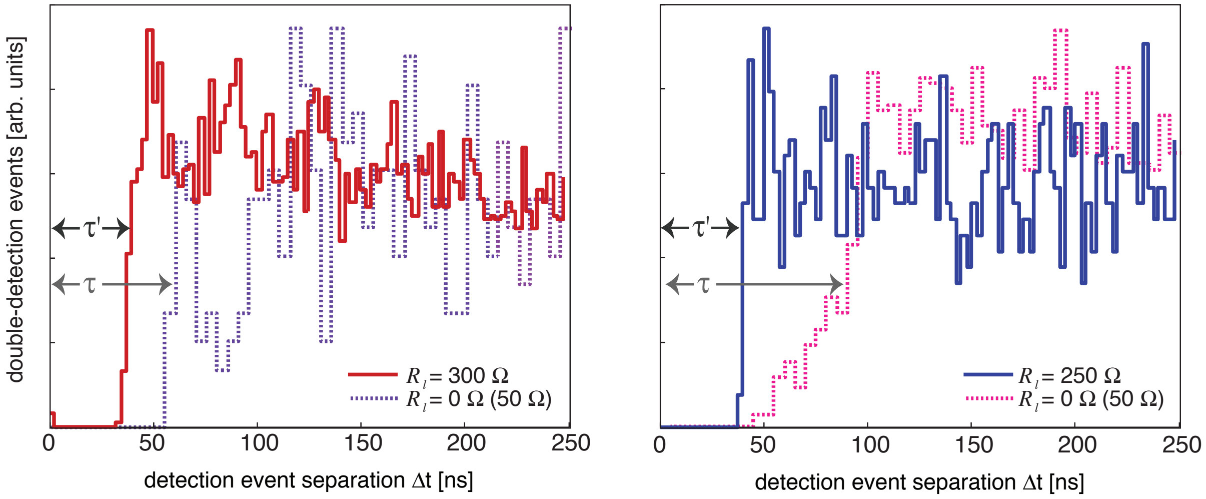


Figure E.4: Detection dead-times. Histograms of detection inter-arrival times for SNSPD 1 and 2 in the left and right panel, respectively. Solid lines correspond to the setup with $R_l = 50\ \Omega$ (given by the impedance of the coaxial cable), while the dashed line shows the result when a $R_l = 350\ \Omega$ resistor is connected to detector 2 inside the cryostat. For R_l=50 Ω we find $\tau \approx 30$ ns for detector 1 and $\tau \approx 100$ ns for detector 2. The dead-time of detector 2 is reduced to around 40 ns when using R_l=350 Ω.

of the detectors [19]. Hence, to allow projections onto the $|\psi^+\rangle$ state using detector 2, the time-bin separation would have to be on the order of 100 ns.

As argued above, it is desirable to reduce the SNSPD dead-time. Previous studies have shown $\tau \propto L_k/R_l$, and as the kinetic inductance is related to the inherent geometry and material properties of the SNSPD (which cannot be easily modified), we focus on increasing R_l as a means of reducing τ [23]. To that end we put a $R_s = 300\ \Omega$ resistor in series with SNSPD detector 2. The resistors are regular ceramic surface-mount resistors and are connected to the SNSPDs after a 10 cm long coaxial cable. The resulting inter-arrival time statistics is plotted as a dashed line in Fig. E.4. We see that the new dead-time of detector 2, τ', is significantly reduced to around 40 ns. The discrepancy between the 7 increase in R_l and the resulting 2.5 decrease in the dead-time is most likely due to uncertainty of the exact value of R_s at low temperatures and limitations on our ability to discriminate subsequent detections due to pulse pile-up. One might conclude that an additional increase of the load resistance would further reduce the dead-time. However, we anticipate that with larger values of R_l the detector would begin to latch (i.e. not return to the superconducting state after the detection of a photon).

E.3 Experimental setup

Our experimental setup is similar to that described in [12]. As depicted in Fig. E.5, a stabilized cw laser emits polarized light at 1550 nm. The light is split by a polarization maintaining finer-optic beam splitter, and travels to two different stations, which we will refer to as Alice (A) and Bob (B). At each station, light is sent through intensity modulators that carve 0.5 ns long pulses, which, after appropriate attenuation, form time-bin qubit states encoded into laser pulses with mean photon number well below one. For instance, $|0\rangle$ corresponds to an attenuated laser pulse in an early temporal mode, $|1\rangle$ corresponds to a laser pulse in a late temporal mode, and $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$ is generated by opening the intensity modulator twice in a row, generating photons in a coherent superposition of early and late temporal modes. The subsequent phase modulator allows applying a π phase shift to the late temporal mode, which results in generating $|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$. Qubits are created at a repetition rate of 5 MHz, and the two temporal modes are separated by 75 ns. Finally, each qubit (one generated at Alice's and one at Bob's) is sent through a polarization controller and 20 km of spooled fiber, which introduce random global phase shifts, and arrive at the Bell state analyzer where the BSM is performed using a beam splitter and two SNSPDs. Detection statistics is collected using a time-to-digital converter for various combinations of mean photon numbers per qubit generated at Alice's and Bob's, and is recorded on a PC.

It is important to recall that, for a BSM, the two photons impinging on the beam splitter must be indistinguishable in all degrees of freedom: polarization, arrival time, and frequency. Frequency indistinguishability is particularly important when working with $|\pm\rangle$ time-bin qubit states, as a frequency difference $\Delta\nu$ translates into a difference $\Delta\phi$ between the phases characterizing the superposition of the two time-bin qubit states according to $\Delta\phi = 2\pi\Delta\nu t_0$, where t_0 denotes the temporal separation between $|0\rangle$ and $|1\rangle$. While a constant phase difference (due to a constant frequency difference) can be compensated for during qubit preparation, having time varying phase differences becomes problematic once the variation of the phase difference exceeds a few degrees. Consequently, the time-bin separation is not only constrained by the dead-time of the detectors, but also by the frequency stability of the light sources (assuming independent sources). For example, for our time-bin separation of t_0=75 ns, the two lasers must be frequency stable at least within $\sim$185 kHz over the duration of a measurement to keep the phase error under 5^o. Unfortunately, lasers with such frequency stability are currently not commercially available. To circumvent this problem, we used only one laser in our experiment, which allowed Alice and Bob to generate time-bin qubits with stable phase relation. Finally, to ensure indistinguishability in polarization and arrival time, we implemented feedback control as described in [12].

E.4 Results

To characterize the reliability and efficiency of our Bell state analyzer, we work within the framework of the measurement-device-independent quantum key distribution (MDI-QKD) protocol [4]. In MDI-QKD two parties, Alice and Bob, prepare qubits that are sent over channels to be projected onto entangled states via a BSM, thus establishing an entangled channel that allows for the generation of a correlated key. Conversely, the possibility to generate highly correlated bits using an MDI-QKD type setup allows

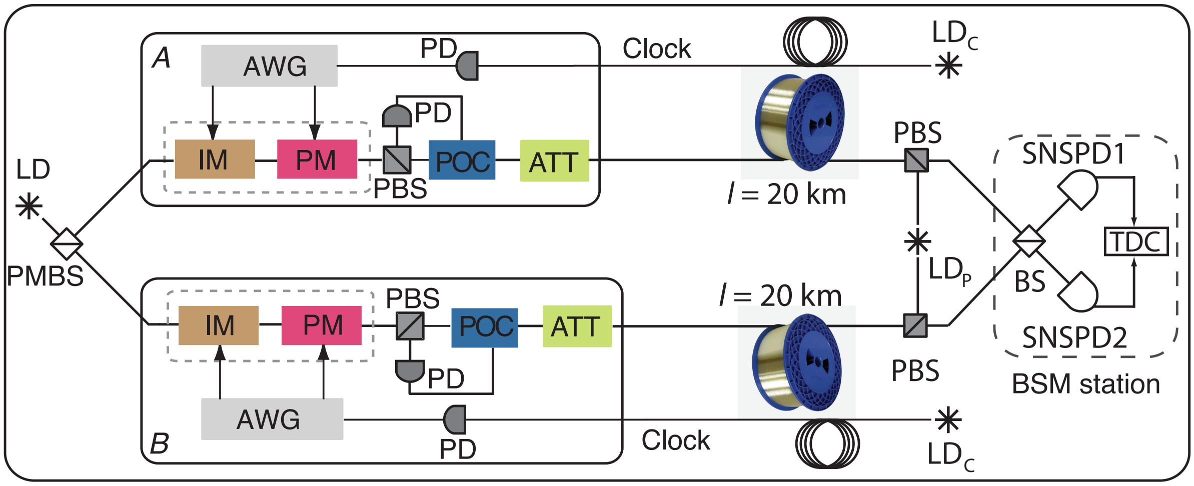


Figure E.5: Schematic of the experimental setup employed for a BSM with time-bin qubits. LD, laser diode; PMBS, polarization maintaining beam splitter; IM, intensity modulator; PM, phase modulator; PBS, polarization beam splitter; POC, polarization controller; PD, photodiode; BS, beam splitter; AWG, arbitrary waveform generator; ATT, variable optical attenuator; SNSPD, superconducting nanowire single-photon detector. The lasers LD$_C$ and LD$_P$ are used for timing and polarization feedback control, respectively, which is further explained in [12].

one to draw conclusions about the quality of the BSM. To demonstrate efficient Bell state measurements with time-bin qubits, Alice and Bob prepare various combinations of qubit states, encoded into attenuated laser pulses with one out of three possible mean photon numbers (0.11, 0.05 and 0) and with both qubits belonging to the same basis i.e. $|\psi\rangle_A , |\psi\rangle_B \in \{|0\rangle , |1\rangle\}$ or $|\psi\rangle_A , |\psi\rangle_B \in \{|+\rangle , |-\rangle\}$, and send them to the Bell state analyzer. We define the z-basis to be spanned by $|0\rangle$ and $|1\rangle$, and the x-basis to be spanned by $|+\rangle$ and $|-\rangle$. For each combination of states and mean photon numbers, we record the number of projections onto $|\psi^+\rangle$ and $|\psi^-\rangle$.

E.4.1 Error rates

An important criterion for assessing the possibility for BSMs with time-bin qubits are error rates, which, for each basis and Bell state, are given by the number of erroneous projections (e.g. projections onto $|\psi^-\rangle$ if the two input states were identical) divided by the total number of projections onto that Bell state. Towards this end, qubits should be encoded into true single photons. As we use attenuated laser pulses instead, which feature Poissonian-distributed photon numbers, we use a decoy state protocol [24] to assess upper bounds e_{11} for the error rates that we *would* have measured *had* we used true single photon inputs. (Here the subscripts 1 refer to the single photon components of the Poissonian photon number distributions) These bounds are calculated from the Bell-state projections measurements using the three above mentioned mean photon numbers and the resulting error rates. The upper bound on the inferred single photon error rates are listed in table E.1 below.

Table E.1: Bounded error rates e_{11}^z and e_{11}^x for two single photon inputs (one at Alice's and one at Bob's) with both photons prepared in the z and x basis, respectively. The rates are extracted from the measured data using a decoy state method [24].

Error rates	Projections onto $\|\psi^-\rangle$ (%)	Projections onto $\|\psi^+\rangle$ (%)
e_{11}^z	0.44±0.07	0.80±0.07
e_{11}^x	3.6±0.8	6.7±0.8

The results are close to ideal, in particular regarding the error rate for the z-basis, which exceeds the ideal outcome of 0% by only 0.44% and 0.80% for projections onto $|\psi^-\rangle$ and $|\psi^+\rangle$, respectively. This is a very good result, especially given that Alice and Bob are separated by 40 km of spooled fiber. The remaining errors are due to (almost negligible) background light leaking through Alice's and Bob's intensity modulators (featuring 50 dB extinction ratio) and detector dark counts (around 10 Hz, including detector counts due to blackbody radiation). For the x-basis, the error rates exceed the ideal outcome of 0% by 3.6% and 6.7% for the $|\psi^-\rangle$ and $|\psi^+\rangle$ projections, respectively. We attribute the increment in the error rates compared to those of the z-basis to phase errors occurring during the preparation of the $|-\rangle$-state. In addition the gap between the bound on e_{11} and its actual value may be larger. This poorer performance of the decoy state analysis is due to errors in the raw data arising from multi-photon contributions (e.g. two photons arriving from Alice and zero photons from Bob) [12], which partially propagate into the calculated bound for e_{11}^{x}.

E.4.2 Efficiency

While error rates allow assessing if the BSM is functioning correctly, an equally important measure is the efficiency of the Bell state analyzer. As in the previous section, we use the decoy state protocol [24] to find a lower bound on the number of projections onto $|\psi^{+}\rangle$ and $|\psi^{-}\rangle$ that originate from the emission of single photons at Alice's and Bob's. The number of such projections per clock cycle, $Q_{11}^{x,z}$ (where x, z denotes the basis in which the qubits have been prepared), then allows us to calculate the BSM efficiency for each basis and Bell state using

$$Q_{11}^{x,z} = P_1(\mu)P_1(\mu)t^2\eta_{BSM}^{x,z}. \tag{E.2}$$

Here, $P_1(\mu)$ refers to the probability of emission of a single photon per (Poissonian distributed) source, t denotes to the transmission between Alice or Bob and the Bell state analyzer, and $\eta_{BSM}^{x,z}$ is the basis-dependent efficiency of the BSM. The results for η_{BSM} are listed in table E.2.

Table E.2: Bell state measurement efficiencies extracted from measured data using a decoy state method [24].

Basis	Efficiency for projections onto $\|\psi^{-}\rangle$ (%)	Efficiency for projections onto $\|\psi^{+}\rangle$ (%)	Total efficiency (%)
z	13.6±0.2	14.5±0.2	28.1±0.4
x	14.5±0.4	15.3±0.4	29.8±0.8

We note, first, that the values for the total efficiencies per basis differ by only 1.7%, confirming that we can perform all projections with almost equal probability. In particular, this shows that the detectors have indeed fully recovered after 75 ns. Second, we find that the efficiency averaged over the x, y and z bases (where we made the physically motivated assumption that the efficiency in the y-basis, which we did not measure, equals the one measured in the x-basis), η_{BSM}, corresponds to that estimated using Eq.E.1 and taking into account the measured detector quantum efficiencies:

$$\begin{aligned} \eta_{BSM} &= \frac{1}{3}\big(\eta_{bsm,z} + 2\eta_{bsm,x}\big) = (29.3 \pm 0.4)\% \\ &\approx \frac{1}{2}\eta_{det}^2 = \big(29.5 \pm 0.4\big)\%. \end{aligned} \tag{E.3}$$

Furthermore, we point out that the efficiency is a factor of ≈ 30 higher than what has previously been obtained with time-bin qubits. Finally, we note that our average BSM efficiency is only 2.3% below the theoretical maximum of 5/16≈31% (assuming detectors with 100% efficiency) achievable with previously implemented schemes [17].

E.5 Conclusions and Outlook

We have described and demonstrated how to perform efficient Bell state analysis with time-bin qubits using linear optics and no additional photons. By employing SNSPDs with short dead-times, it is possible to project not only onto the $|\psi^-\rangle$, but also onto the $|\psi^+\rangle$ Bell state. Together with the high quantum efficiency of the SNSPDs, this improved the efficiency of Bell state measurements with time-bin qubits from ≈1% to ≈29%, which falls only a few percent short of the previous theoretical maximum of 31%. With further improvements to reduce photon loss in the transmission line the intrinsic greater than 90% system efficiency of SNSPDs [21] would lead to a Bell state measurement efficiency above 40% and thus approaching the 50% optimum. Additionally, the low noise of the superconducting detectors yields a very small error rate.

Bell state measurements are key ingredients for applications of quantum information processing, including linear optics quantum computing, quantum repeaters, and measurement-device-independent quantum key distribution, and our results are interesting in view of improving (or allowing) implementations. However, to take full advantage of the increased efficiency, detector dead-times need to be decreased, for instance using detector arrays [25], to allow reducing the spacing between temporal modes used to encode time-bin qubits. Shorter time-bin separations would furthermore reduce the requirement on laser stability and enable two independent sources at Alice and Bob employing commercially available lasers.

Acknowledgements

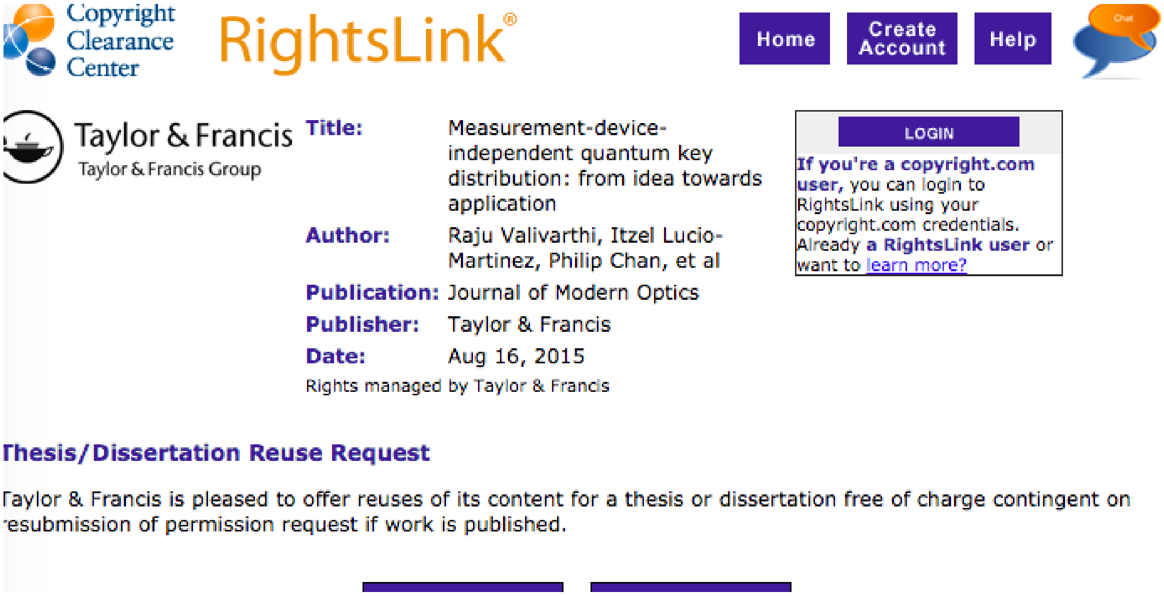
WT, JAS, PC, AR, RV, ILM and DO thank Neil Sinclair and Vladimir Kiselyov for discussions and technical support, and acknowledge funding by Alberta Innovates Technology Futures (AITF), the National Sciences and Engineering Research Council of Canada (NSERC), the US Defense Advanced Research Projects Agency (DARPA) Quiness Program under Grant No. W31P4Q-13-1-0004, and the Killam Trusts. VBV and SWN acknowledge partial funding for detector development from the DARPA Information in a Photon (InPho) program. Part of the research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

Appendix F

Copyright permissions

This appendix states the copyright permissions required to include Papers 1-5 in this thesis. Papers 1,2,4,5 are published in journals that grant me permission to use these papers in my thesis. Proof of this permission is shown via screen-shots from the appropriate websites. Paper 2 is uploaded to a pre-print server where only a ?right to distribute? is granted and not a copyright as is the case with journals; a screen-shot is included that describes this. Permission from co-authors has been granted via e-mail communication. Copies of these emails are shown.

F.1 Journals



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

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

Publication: Journal of Modern Optics

Publisher: Taylor & Francis

Date: Aug 16, 2015

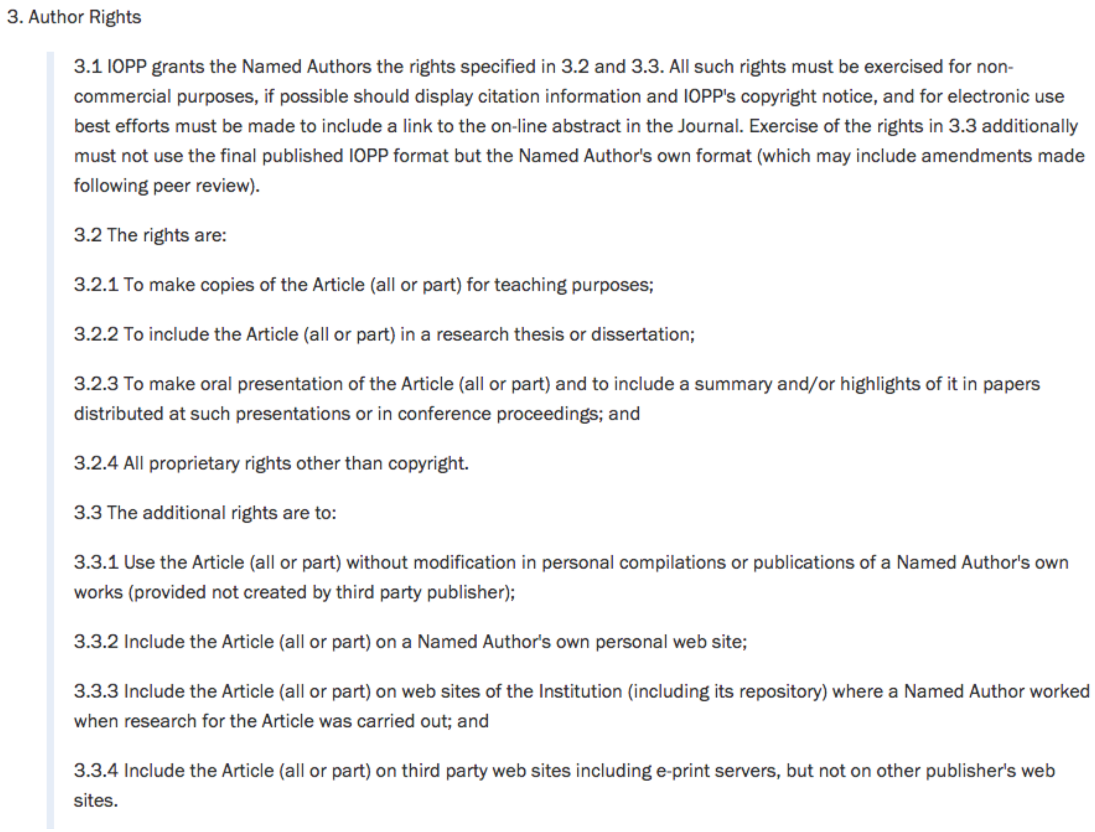
Rights managed by Taylor & Francis

If you're a copyright.com user, you can login to RightsLink using your copyright.com credentials. Already **a RightsLink user** or want to learn more?

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.

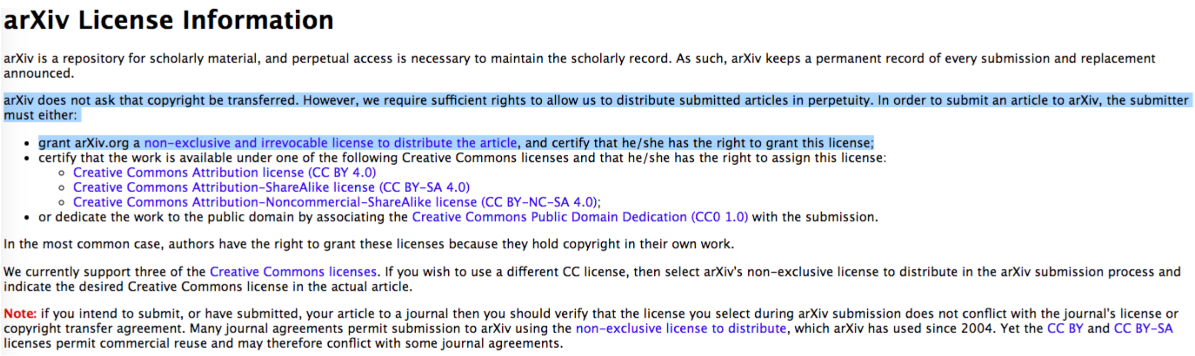
Figure F.1: Copyright permissions for Paper I published in Journal of Modern optics which is under Taylor & Francis Group of journals.



3. Author Rights

> 3.1 IOPP grants the Named Authors the rights specified in 3.2 and 3.3. All such rights must be exercised for non-commercial purposes, if possible should display citation information and IOPP's copyright notice, and for electronic use best efforts must be made to include a link to the on-line abstract in the Journal. Exercise of the rights in 3.3 additionally must not use the final published IOPP format but the Named Author's own format (which may include amendments made following peer review).
>
> 3.2 The rights are:
>
> 3.2.1 To make copies of the Article (all or part) for teaching purposes;
>
> 3.2.2 To include the Article (all or part) in a research thesis or dissertation;
>
> 3.2.3 To make oral presentation of the Article (all or part) and to include a summary and/or highlights of it in papers distributed at such presentations or in conference proceedings; and
>
> 3.2.4 All proprietary rights other than copyright.
>
> 3.3 The additional rights are to:
>
> 3.3.1 Use the Article (all or part) without modification in personal compilations or publications of a Named Author's own works (provided not created by third party publisher);
>
> 3.3.2 Include the Article (all or part) on a Named Author's own personal web site;
>
> 3.3.3 Include the Article (all or part) on web sites of the Institution (including its repository) where a Named Author worked when research for the Article was carried out; and
>
> 3.3.4 Include the Article (all or part) on third party web sites including e-print servers, but not on other publisher's web sites.

Figure F.2: Copyright permissions for Paper II published in Quantum science and technology, a journal of the Institute of Physics (IOP).



arXiv License Information

arXiv is a repository for scholarly material, and perpetual access is necessary to maintain the scholarly record. As such, arXiv keeps a permanent record of every submission and replacement announced.

arXiv does not ask that copyright be transferred. However, we require sufficient rights to allow us to distribute submitted articles in perpetuity. In order to submit an article to arXiv, the submitter must either:

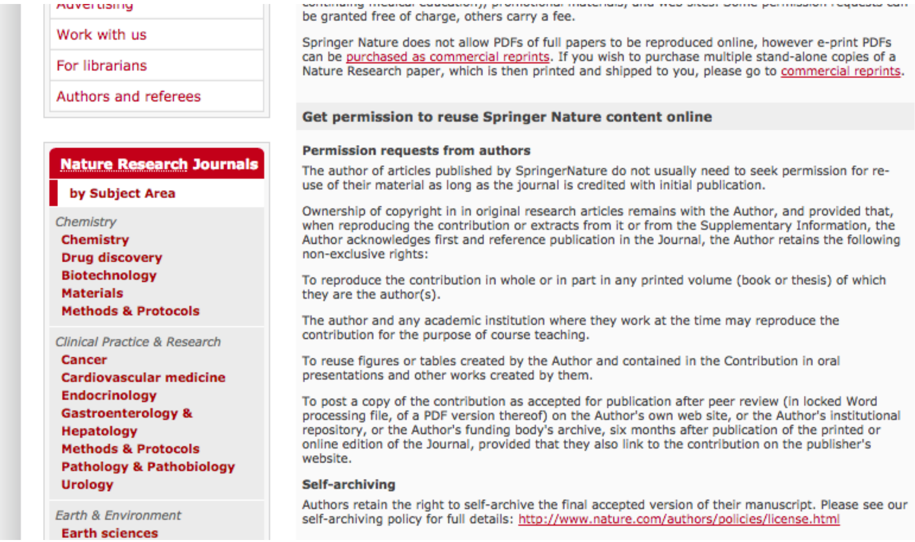
- grant arXiv.org a non-exclusive and irrevocable license to distribute the article, and certify that he/she has the right to grant this license;
- certify that the work is available under one of the following Creative Commons licenses and that he/she has the right to assign this license:
  - Creative Commons Attribution license (CC BY 4.0)
  - Creative Commons Attribution-ShareAlike license (CC BY-SA 4.0)
  - Creative Commons Attribution-Noncommercial-ShareAlike license (CC BY-NC-SA 4.0);
- or dedicate the work to the public domain by associating the Creative Commons Public Domain Dedication (CC0 1.0) with the submission.

In the most common case, authors have the right to grant these licenses because they hold copyright in their own work.

We currently support three of the Creative Commons licenses. If you wish to use a different CC license, then select arXiv's non-exclusive license to distribute in the arXiv submission process and indicate the desired Creative Commons license in the actual article.

Note: if you intend to submit, or have submitted, your article to a journal then you should verify that the license you select during arXiv submission does not conflict with the journal's license or copyright transfer agreement. Many journal agreements permit submission to arXiv using the non-exclusive license to distribute, which arXiv has used since 2004. Yet the CC BY and CC BY-SA licenses permit commercial reuse and may therefore conflict with some journal agreements.

Figure F.3: Copyright permissions for Paper III uploaded in arXiv.



continuing medical education), promotional materials, and web sites. Some permission requests can be granted free of charge, others carry a fee.

Springer Nature does not allow PDFs of full papers to be reproduced online, however e-print PDFs can be purchased as commercial reprints. If you wish to purchase multiple stand-alone copies of a Nature Research paper, which is then printed and shipped to you, please go to commercial reprints.

Get permission to reuse Springer Nature content online

Permission requests from authors

The author of articles published by SpringerNature do not usually need to seek permission for re-use of their material as long as the journal is credited with initial publication.

Ownership of copyright in in original research articles remains with the Author, and provided that, when reproducing the contribution or extracts from it or from the Supplementary Information, the Author acknowledges first and reference publication in the Journal, the Author retains the following non-exclusive rights:

To reproduce the contribution in whole or in part in any printed volume (book or thesis) of which they are the author(s).

The author and any academic institution where they work at the time may reproduce the contribution for the purpose of course teaching.

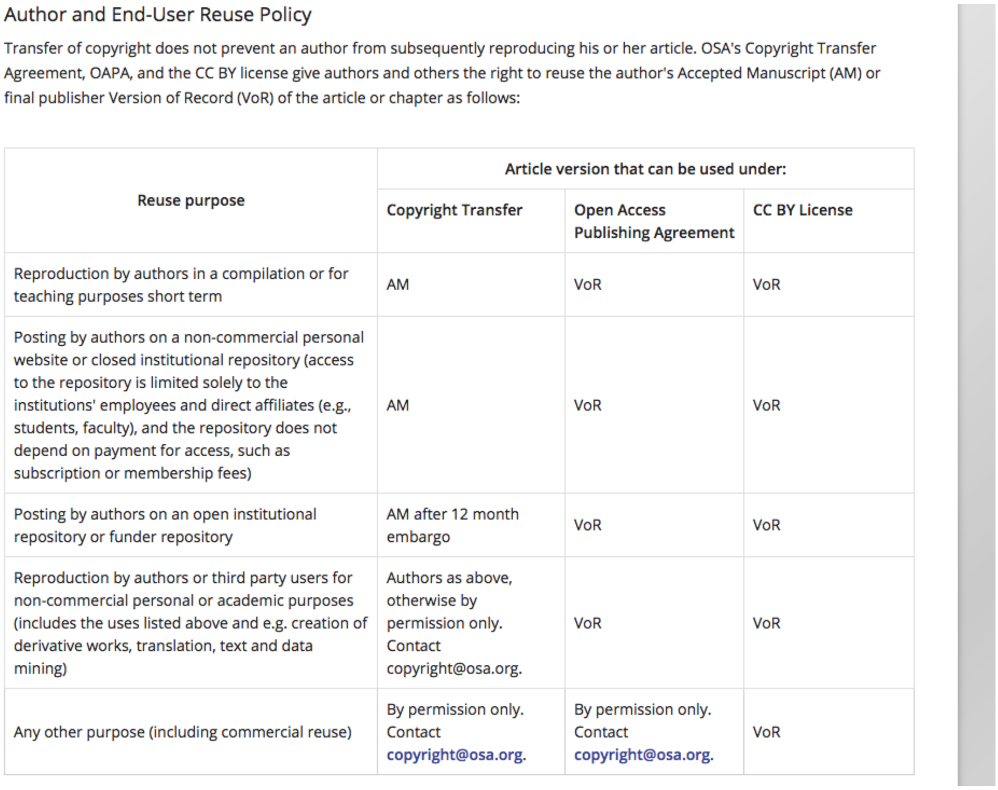
To reuse figures or tables created by the Author and contained in the Contribution in oral presentations and other works created by them.

To post a copy of the contribution as accepted for publication after peer review (in locked Word processing file, of a PDF version thereof) on the Author's own web site, or the Author's institutional repository, or the Author's funding body's archive, six months after publication of the printed or online edition of the Journal, provided that they also link to the contribution on the publisher's website.

Self-archiving

Authors retain the right to self-archive the final accepted version of their manuscript. Please see our self-archiving policy for full details: http://www.nature.com/authors/policies/license.html

Figure F.4: Copyright permissions for Paper IV published in Nature Photonics, a journal of Nature group.



Author and End-User Reuse Policy

Transfer of copyright does not prevent an author from subsequently reproducing his or her article. OSA's Copyright Transfer Agreement, OAPA, and the CC BY license give authors and others the right to reuse the author's Accepted Manuscript (AM) or final publisher Version of Record (VoR) of the article or chapter as follows:

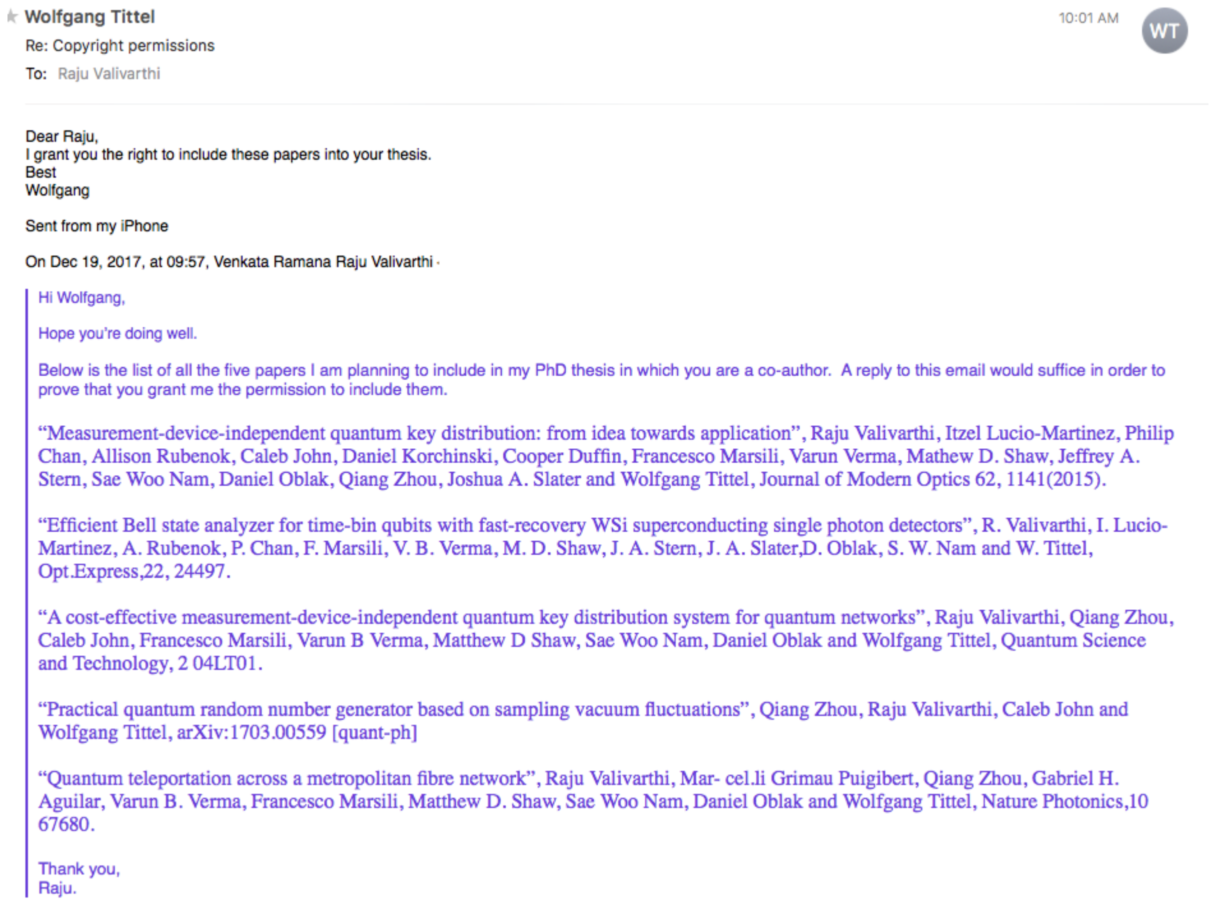
Reuse purpose	**Article version that can be used under:**		
	Copyright Transfer	**Open Access Publishing Agreement**	**CC BY License**
Reproduction by authors in a compilation or for teaching purposes short term	AM	VoR	VoR
Posting by authors on a non-commercial personal website or closed institutional repository (access to the repository is limited solely to the institutions' employees and direct affiliates (e.g., students, faculty), and the repository does not depend on payment for access, such as subscription or membership fees)	AM	VoR	VoR
Posting by authors on an open institutional repository or funder repository	AM after 12 month embargo	VoR	VoR
Reproduction by authors or third party users for non-commercial personal or academic purposes (includes the uses listed above and e.g. creation of derivative works, translation, text and data mining)	Authors as above, otherwise by permission only. Contact copyright@osa.org.	VoR	VoR
Any other purpose (including commercial reuse)	By permission only. Contact **copyright@osa.org**.	By permission only. Contact **copyright@osa.org**.	VoR

Figure F.5: Copyright permissions for Paper V published in Optics Express, a journal of Optical society of America (OSA).

F.2 Co-authors

Co-author list

- W. Tittel
- D. Oblak
- G. H. Aguilar
- M. G. Puigibert
- Qiang Zhou
- Itzel Martinez
- Joshua Slater
- V. B. Verma
- M. D. Shaw
- S. W. Nam
- F. Marsili
- Caleb John
- Cooper Duffin
- Daniel Korchinski
- Allison Rubenok



Wolfgang Tittel

10:01 AM

Re: Copyright permissions

To: Raju Valivarthi

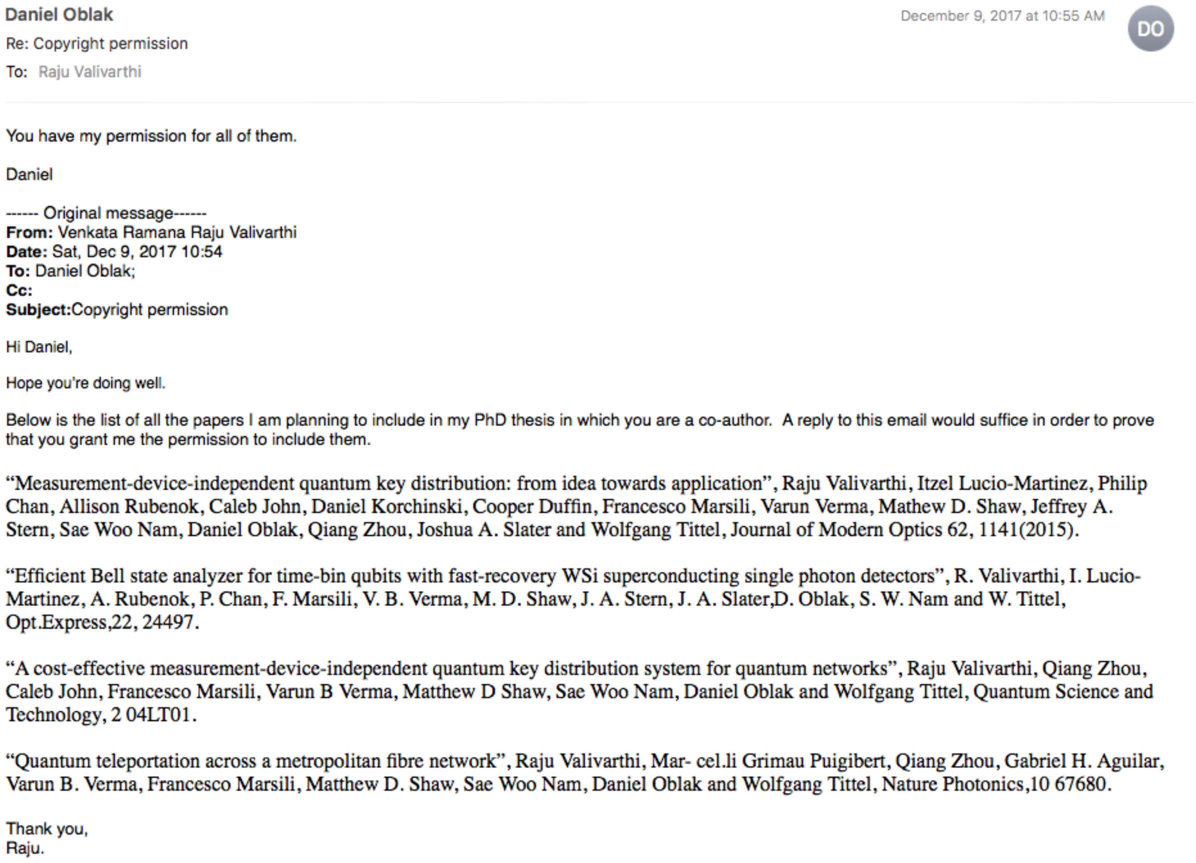
Dear Raju,
I grant you the right to include these papers into your thesis.
Best
Wolfgang

Sent from my iPhone

On Dec 19, 2017, at 09:57, Venkata Ramana Raju Valivarthi

> Hi Wolfgang,
>
> Hope you're doing well.
>
> Below is the list of all the five papers I am planning to include in my PhD thesis in which you are a co-author. A reply to this email would suffice in order to prove that you grant me the permission to include them.
>
> "Measurement-device-independent quantum key distribution: from idea towards application", Raju Valivarthi, Itzel Lucio-Martinez, Philip Chan, Allison Rubenok, Caleb John, Daniel Korchinski, Cooper Duffin, Francesco Marsili, Varun Verma, Mathew D. Shaw, Jeffrey A. Stern, Sae Woo Nam, Daniel Oblak, Qiang Zhou, Joshua A. Slater and Wolfgang Tittel, Journal of Modern Optics 62, 1141(2015).
>
> "Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors", 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, Opt.Express,22, 24497.
>
> "A cost-effective measurement-device-independent quantum key distribution system for quantum networks", Raju Valivarthi, Qiang Zhou, Caleb John, Francesco Marsili, Varun B Verma, Matthew D Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Quantum Science and Technology, 2 04LT01.
>
> "Practical quantum random number generator based on sampling vacuum fluctuations", Qiang Zhou, Raju Valivarthi, Caleb John and Wolfgang Tittel, arXiv:1703.00559 [quant-ph]
>
> "Quantum teleportation across a metropolitan fibre network", Raju Valivarthi, Mar- cel.li Grimau Puigibert, Qiang Zhou, Gabriel H. Aguilar, Varun B. Verma, Francesco Marsili, Matthew D. Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Nature Photonics,10 67680.
>
> Thank you,
> Raju.

Figure F.6: Copyright permissions from Prof. Wolfgang Tittel.



Daniel Oblak
Re: Copyright permission
To: Raju Valivarthi

December 9, 2017 at 10:55 AM

You have my permission for all of them.

Daniel

------ Original message------
From: Venkata Ramana Raju Valivarthi
Date: Sat, Dec 9, 2017 10:54
To: Daniel Oblak;
Cc:
Subject: Copyright permission

Hi Daniel,

Hope you're doing well.

Below is the list of all the papers I am planning to include in my PhD thesis in which you are a co-author. A reply to this email would suffice in order to prove that you grant me the permission to include them.

"Measurement-device-independent quantum key distribution: from idea towards application", Raju Valivarthi, Itzel Lucio-Martinez, Philip Chan, Allison Rubenok, Caleb John, Daniel Korchinski, Cooper Duffin, Francesco Marsili, Varun Verma, Mathew D. Shaw, Jeffrey A. Stern, Sae Woo Nam, Daniel Oblak, Qiang Zhou, Joshua A. Slater and Wolfgang Tittel, Journal of Modern Optics 62, 1141(2015).

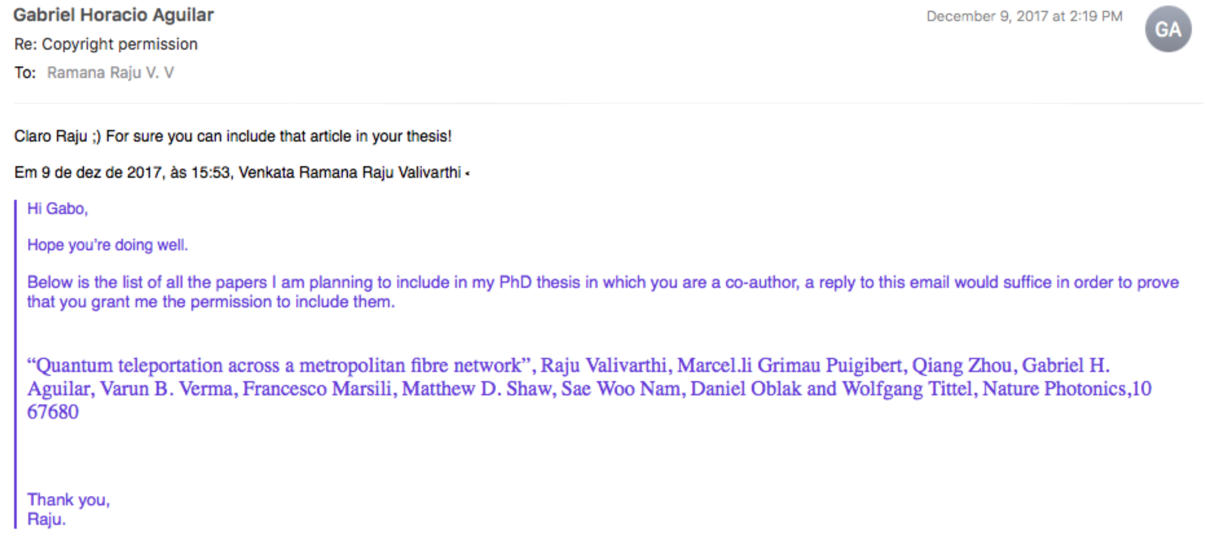
"Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors", R. Valivarthi, I. Lucio-Martinez, A. Rubenok, P. Chan, F. Marsili, V. B. Verma, M. D. Shaw, J. A. Stern, J. A. Slater,D. Oblak, S. W. Nam and W. Tittel, Opt.Express,22, 24497.

"A cost-effective measurement-device-independent quantum key distribution system for quantum networks", Raju Valivarthi, Qiang Zhou, Caleb John, Francesco Marsili, Varun B Verma, Matthew D Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Quantum Science and Technology, 2 04LT01.

"Quantum teleportation across a metropolitan fibre network", Raju Valivarthi, Mar- cel.li Grimau Puigibert, Qiang Zhou, Gabriel H. Aguilar, Varun B. Verma, Francesco Marsili, Matthew D. Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Nature Photonics,10 67680.

Thank you,
Raju.

Figure F.7: Copyright permissions from Daniel Oblak.



Gabriel Horacio Aguilar

Re: Copyright permission

To: Ramana Raju V. V

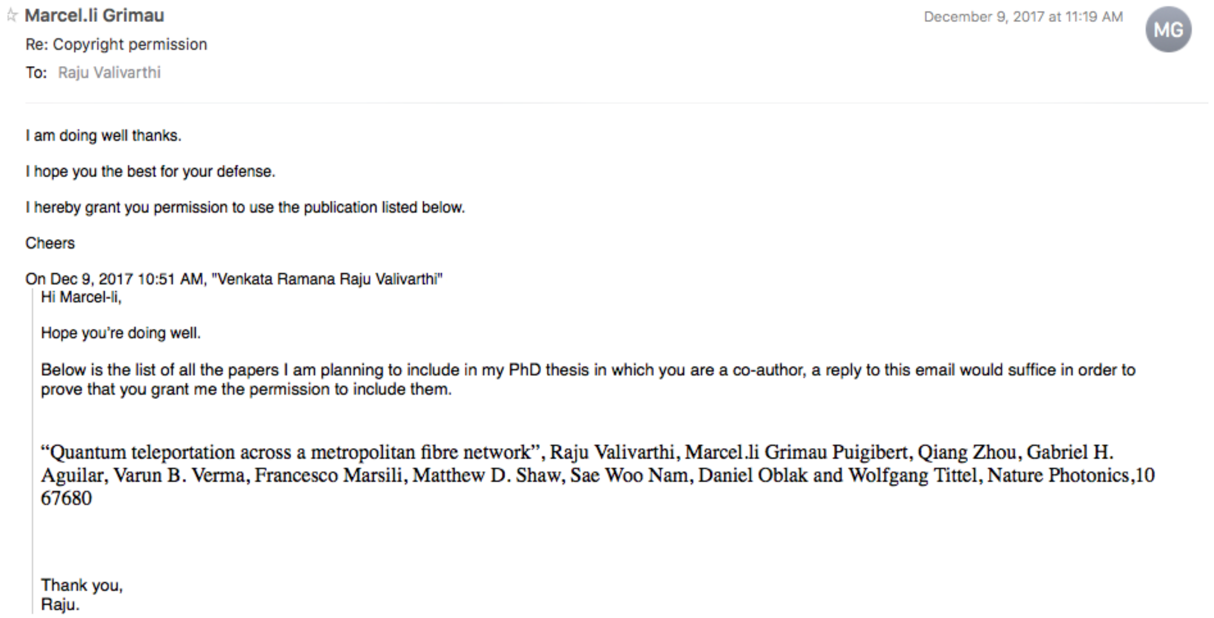
December 9, 2017 at 2:19 PM

Claro Raju ;) For sure you can include that article in your thesis!

Em 9 de dez de 2017, às 15:53, Venkata Ramana Raju Valivarthi ‹

> Hi Gabo,
>
> Hope you're doing well.
>
> Below is the list of all the papers I am planning to include in my PhD thesis in which you are a co-author, a reply to this email would suffice in order to prove that you grant me the permission to include them.
>
> “Quantum teleportation across a metropolitan fibre network”, Raju Valivarthi, Marcel.li Grimau Puigibert, Qiang Zhou, Gabriel H. Aguilar, Varun B. Verma, Francesco Marsili, Matthew D. Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Nature Photonics,10 67680
>
> Thank you,
> Raju.

Figure F.8: Copyright permissions from Gabriel Aguilar.



Marcel.li Grimau

Re: Copyright permission

To: Raju Valivarthi

December 9, 2017 at 11:19 AM

I am doing well thanks.

I hope you the best for your defense.

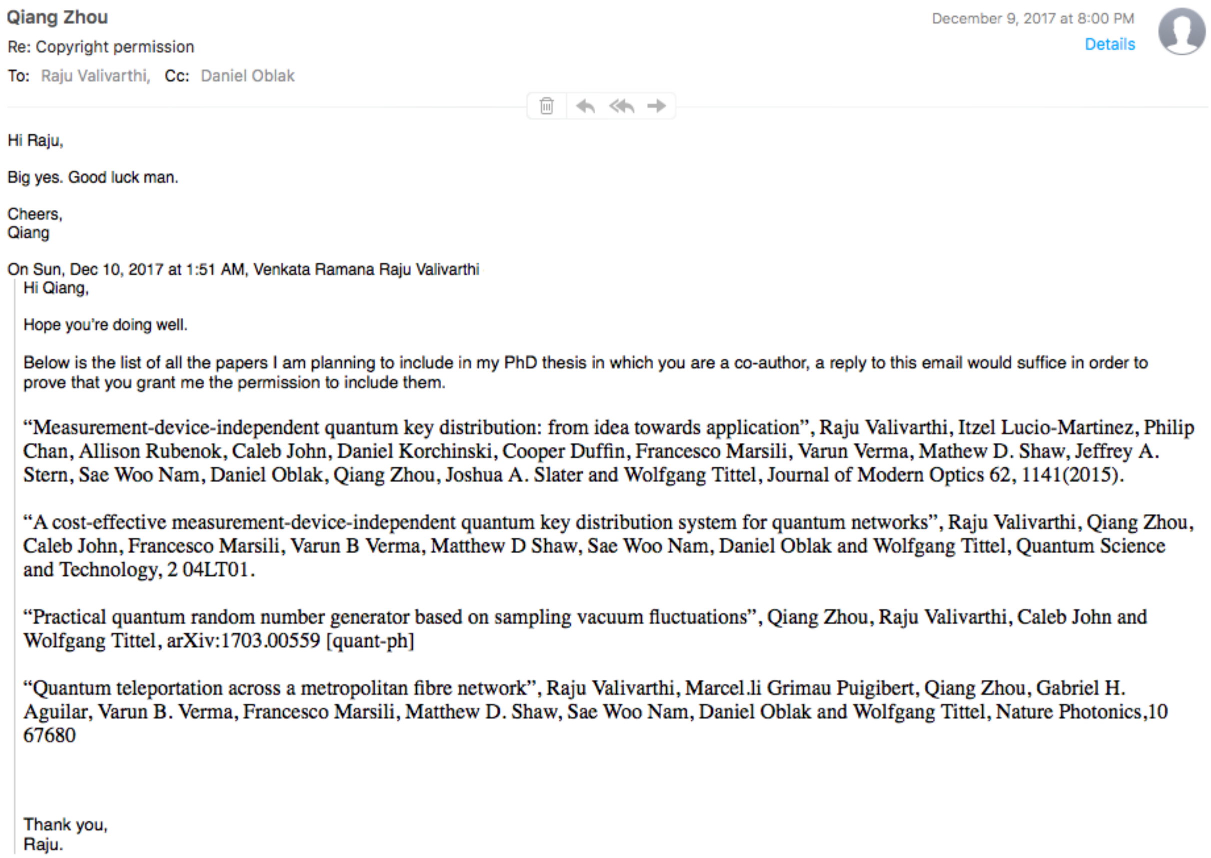
I hereby grant you permission to use the publication listed below.

Cheers

On Dec 9, 2017 10:51 AM, "Venkata Ramana Raju Valivarthi"

> Hi Marcel-li,
>
> Hope you're doing well.
>
> Below is the list of all the papers I am planning to include in my PhD thesis in which you are a co-author, a reply to this email would suffice in order to prove that you grant me the permission to include them.
>
> “Quantum teleportation across a metropolitan fibre network”, Raju Valivarthi, Marcel.li Grimau Puigibert, Qiang Zhou, Gabriel H. Aguilar, Varun B. Verma, Francesco Marsili, Matthew D. Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Nature Photonics,10 67680
>
> Thank you,
> Raju.

Figure F.9: Copyright permissions from Marcel-li Grimau Puigibert.



Qiang Zhou
Re: Copyright permission
To: Raju Valivarthi, Cc: Daniel Oblak

December 9, 2017 at 8:00 PM

Hi Raju,

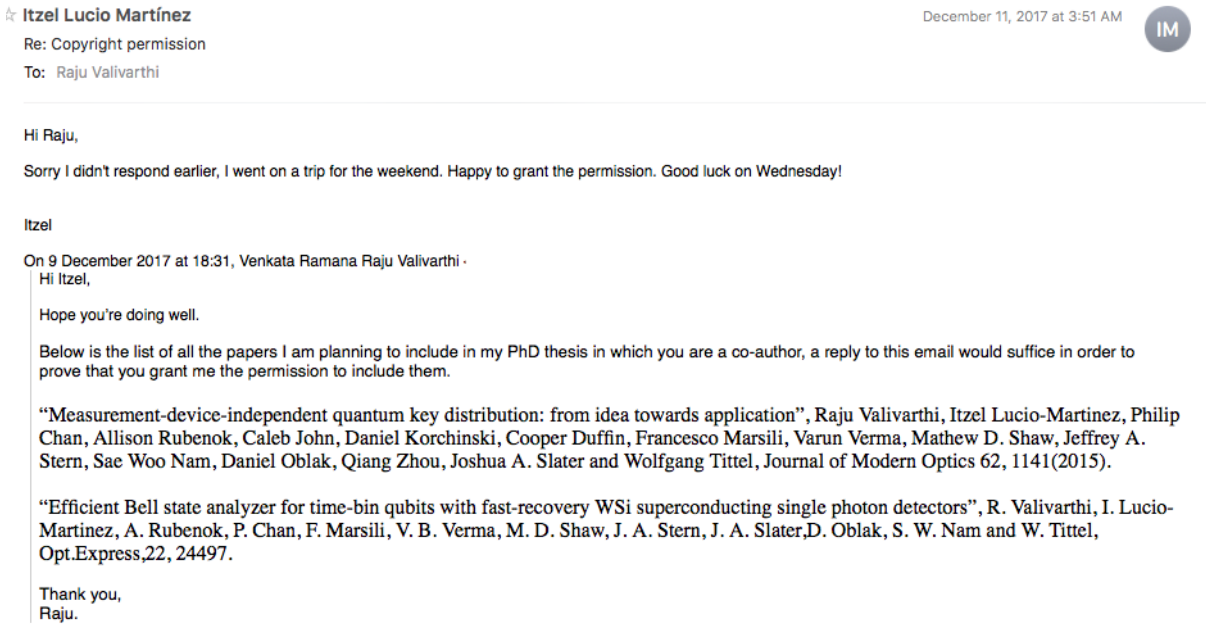
Big yes. Good luck man.

Cheers,
Qiang

On Sun, Dec 10, 2017 at 1:51 AM, Venkata Ramana Raju Valivarthi

> Hi Qiang,
>
> Hope you're doing well.
>
> Below is the list of all the papers I am planning to include in my PhD thesis in which you are a co-author, a reply to this email would suffice in order to prove that you grant me the permission to include them.
>
> "Measurement-device-independent quantum key distribution: from idea towards application", Raju Valivarthi, Itzel Lucio-Martinez, Philip Chan, Allison Rubenok, Caleb John, Daniel Korchinski, Cooper Duffin, Francesco Marsili, Varun Verma, Mathew D. Shaw, Jeffrey A. Stern, Sae Woo Nam, Daniel Oblak, Qiang Zhou, Joshua A. Slater and Wolfgang Tittel, Journal of Modern Optics 62, 1141(2015).
>
> "A cost-effective measurement-device-independent quantum key distribution system for quantum networks", Raju Valivarthi, Qiang Zhou, Caleb John, Francesco Marsili, Varun B Verma, Matthew D Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Quantum Science and Technology, 2 04LT01 .
>
> "Practical quantum random number generator based on sampling vacuum fluctuations", Qiang Zhou, Raju Valivarthi, Caleb John and Wolfgang Tittel, arXiv:1703.00559 [quant-ph]
>
> "Quantum teleportation across a metropolitan fibre network", Raju Valivarthi, Marcel.li Grimau Puigibert, Qiang Zhou, Gabriel H. Aguilar, Varun B. Verma, Francesco Marsili, Matthew D. Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Nature Photonics,10 67680
>
> Thank you,
> Raju.

Figure F.10: Copyright permissions from Qiang Zhou.



☆ **Itzel Lucio Martínez**

Re: Copyright permission

To: Raju Valivarthi

December 11, 2017 at 3:51 AM

Hi Raju,

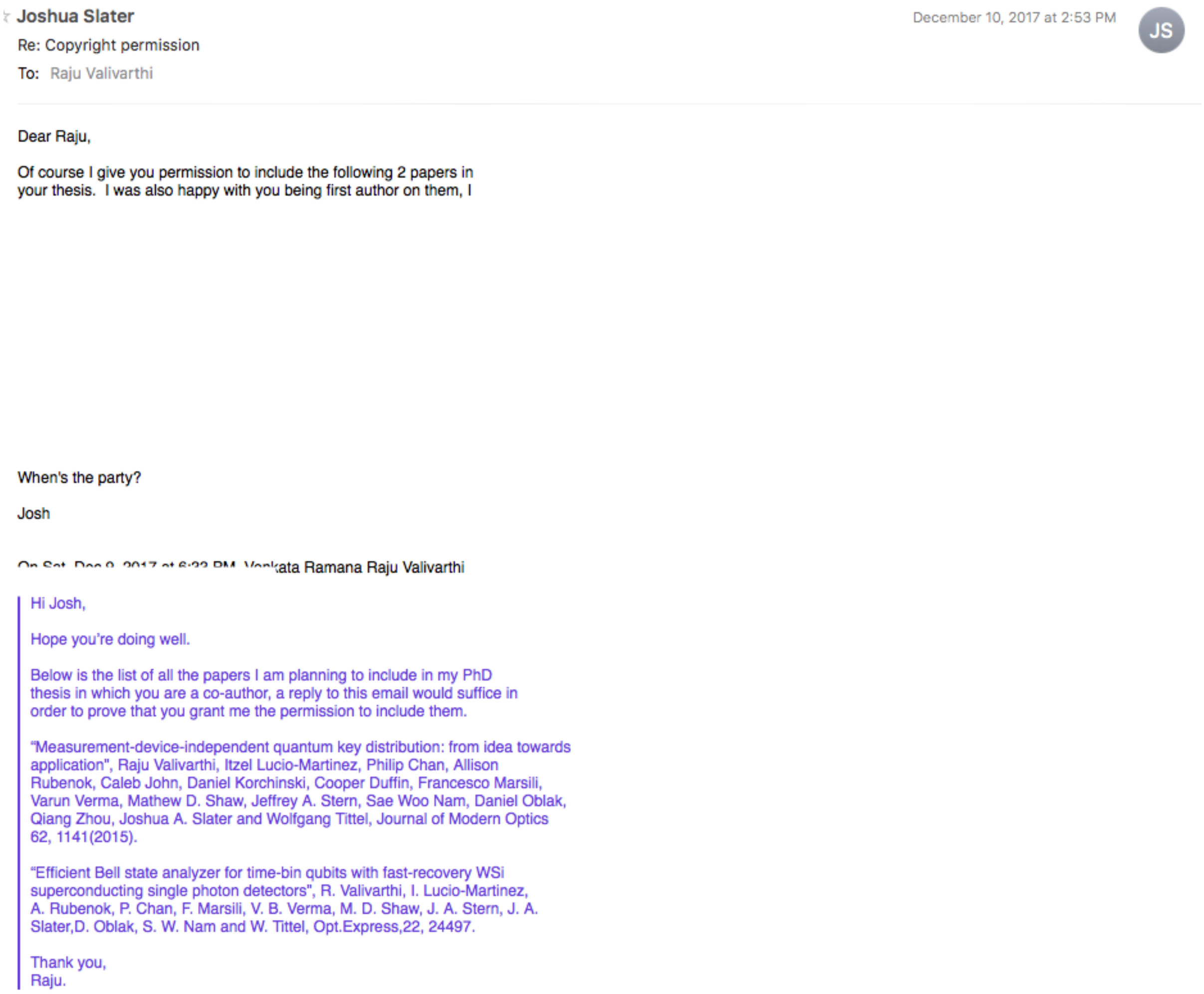
Sorry I didn't respond earlier, I went on a trip for the weekend. Happy to grant the permission. Good luck on Wednesday!

Itzel

On 9 December 2017 at 18:31, Venkata Ramana Raju Valivarthi ·

> Hi Itzel,
>
> Hope you're doing well.
>
> Below is the list of all the papers I am planning to include in my PhD thesis in which you are a co-author, a reply to this email would suffice in order to prove that you grant me the permission to include them.
>
> "Measurement-device-independent quantum key distribution: from idea towards application", Raju Valivarthi, Itzel Lucio-Martinez, Philip Chan, Allison Rubenok, Caleb John, Daniel Korchinski, Cooper Duffin, Francesco Marsili, Varun Verma, Mathew D. Shaw, Jeffrey A. Stern, Sae Woo Nam, Daniel Oblak, Qiang Zhou, Joshua A. Slater and Wolfgang Tittel, Journal of Modern Optics 62, 1141(2015).
>
> "Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors", 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, Opt.Express,22, 24497.
>
> Thank you,
> Raju.

Figure F.11: Copyright permissions from Itzel Lucio-Martinez.



Joshua Slater
Re: Copyright permission
To: Raju Valivarthi

December 10, 2017 at 2:53 PM

Dear Raju,

Of course I give you permission to include the following 2 papers in your thesis. I was also happy with you being first author on them, I

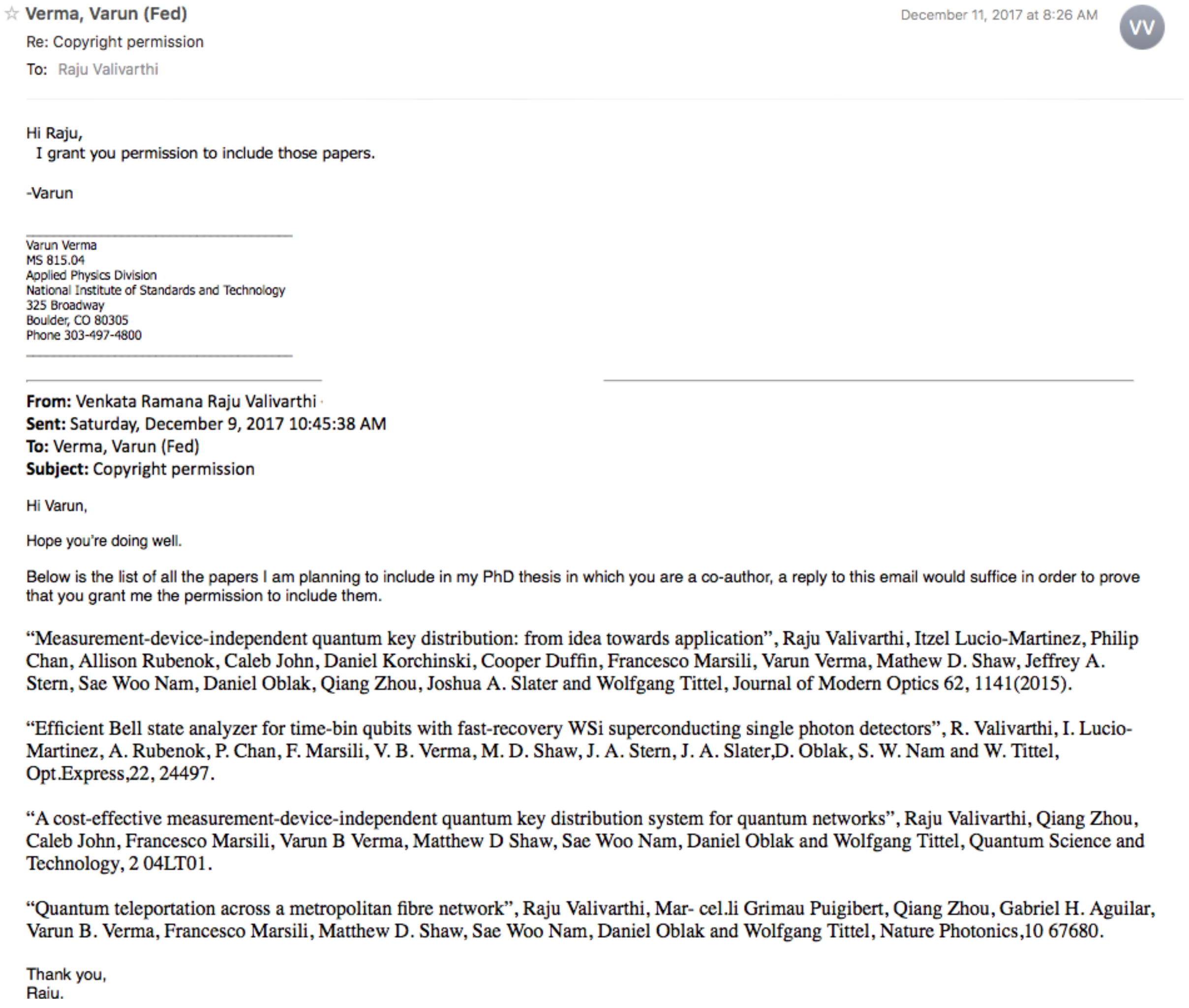
When's the party?

Josh

On Sat, Dec 9, 2017 at 6:33 PM, Venkata Ramana Raju Valivarthi

> Hi Josh,
>
> Hope you're doing well.
>
> Below is the list of all the papers I am planning to include in my PhD thesis in which you are a co-author, a reply to this email would suffice in order to prove that you grant me the permission to include them.
>
> "Measurement-device-independent quantum key distribution: from idea towards application", Raju Valivarthi, Itzel Lucio-Martinez, Philip Chan, Allison Rubenok, Caleb John, Daniel Korchinski, Cooper Duffin, Francesco Marsili, Varun Verma, Mathew D. Shaw, Jeffrey A. Stern, Sae Woo Nam, Daniel Oblak, Qiang Zhou, Joshua A. Slater and Wolfgang Tittel, Journal of Modern Optics 62, 1141(2015).
>
> "Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors", 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, Opt.Express,22, 24497.
>
> Thank you,
> Raju.

Figure F.12: Copyright permissions from Joshua Slater.



☆ **Verma, Varun (Fed)**

December 11, 2017 at 8:26 AM

Re: Copyright permission

To: Raju Valivarthi

Hi Raju,
I grant you permission to include those papers.

-Varun

Varun Verma
MS 815.04
Applied Physics Division
National Institute of Standards and Technology
325 Broadway
Boulder, CO 80305
Phone 303-497-4800

From: Venkata Ramana Raju Valivarthi
Sent: Saturday, December 9, 2017 10:45:38 AM
To: Verma, Varun (Fed)
Subject: Copyright permission

Hi Varun,

Hope you're doing well.

Below is the list of all the papers I am planning to include in my PhD thesis in which you are a co-author, a reply to this email would suffice in order to prove that you grant me the permission to include them.

"Measurement-device-independent quantum key distribution: from idea towards application", Raju Valivarthi, Itzel Lucio-Martinez, Philip Chan, Allison Rubenok, Caleb John, Daniel Korchinski, Cooper Duffin, Francesco Marsili, Varun Verma, Mathew D. Shaw, Jeffrey A. Stern, Sae Woo Nam, Daniel Oblak, Qiang Zhou, Joshua A. Slater and Wolfgang Tittel, Journal of Modern Optics 62, 1141(2015).

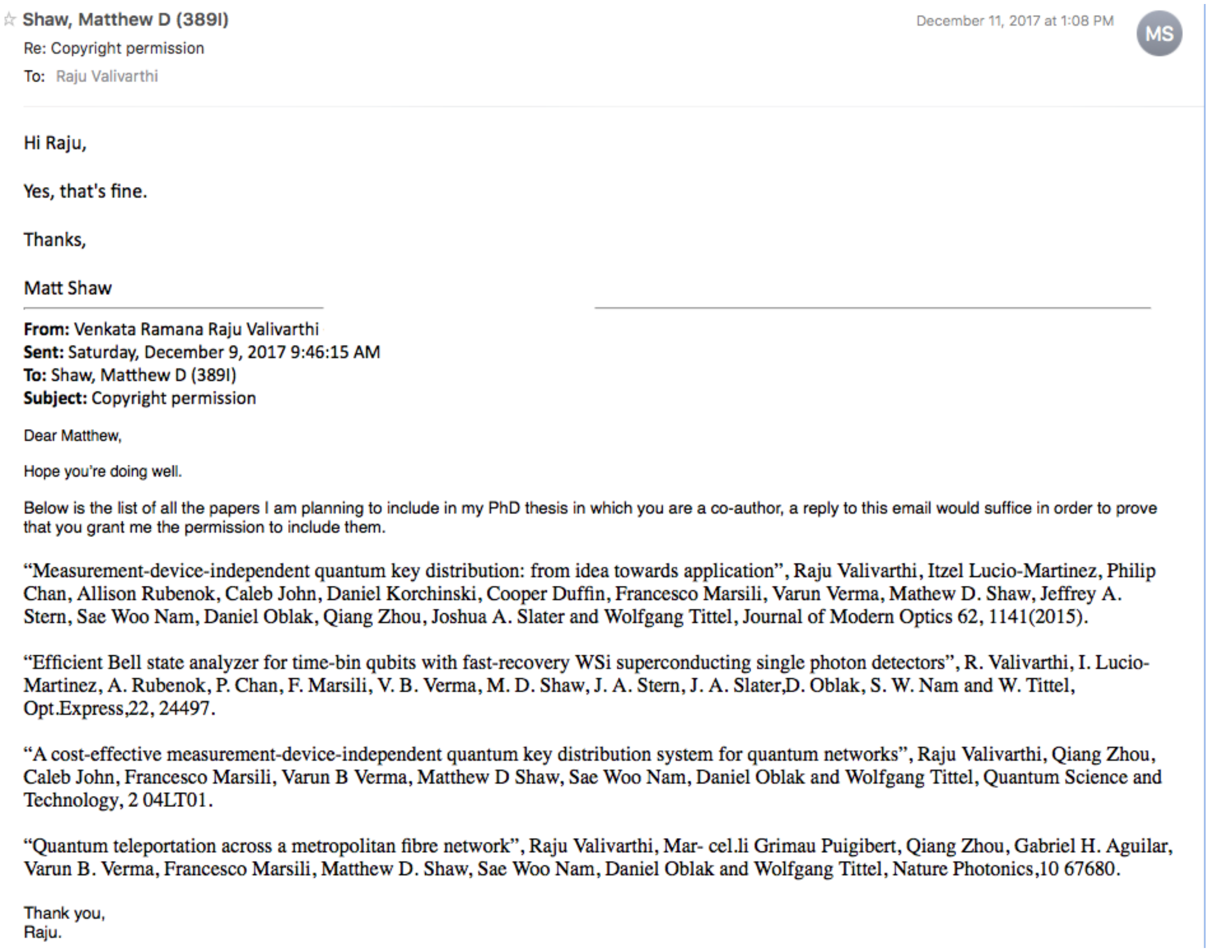
"Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors", R. Valivarthi, I. Lucio-Martinez, A. Rubenok, P. Chan, F. Marsili, V. B. Verma, M. D. Shaw, J. A. Stern, J. A. Slater,D. Oblak, S. W. Nam and W. Tittel, Opt.Express,22, 24497.

"A cost-effective measurement-device-independent quantum key distribution system for quantum networks", Raju Valivarthi, Qiang Zhou, Caleb John, Francesco Marsili, Varun B Verma, Matthew D Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Quantum Science and Technology, 2 04LT01.

"Quantum teleportation across a metropolitan fibre network", Raju Valivarthi, Mar- cel.li Grimau Puigibert, Qiang Zhou, Gabriel H. Aguilar, Varun B. Verma, Francesco Marsili, Matthew D. Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Nature Photonics,10 67680.

Thank you,
Raju.

Figure F.13: Copyright permissions from Varun verma.



☆ **Shaw, Matthew D (389I)**
Re: Copyright permission
To: Raju Valivarthi

December 11, 2017 at 1:08 PM

Hi Raju,

Yes, that's fine.

Thanks,

Matt Shaw

From: Venkata Ramana Raju Valivarthi
Sent: Saturday, December 9, 2017 9:46:15 AM
To: Shaw, Matthew D (389I)
Subject: Copyright permission

Dear Matthew,

Hope you're doing well.

Below is the list of all the papers I am planning to include in my PhD thesis in which you are a co-author, a reply to this email would suffice in order to prove that you grant me the permission to include them.

"Measurement-device-independent quantum key distribution: from idea towards application", Raju Valivarthi, Itzel Lucio-Martinez, Philip Chan, Allison Rubenok, Caleb John, Daniel Korchinski, Cooper Duffin, Francesco Marsili, Varun Verma, Mathew D. Shaw, Jeffrey A. Stern, Sae Woo Nam, Daniel Oblak, Qiang Zhou, Joshua A. Slater and Wolfgang Tittel, Journal of Modern Optics 62, 1141(2015).

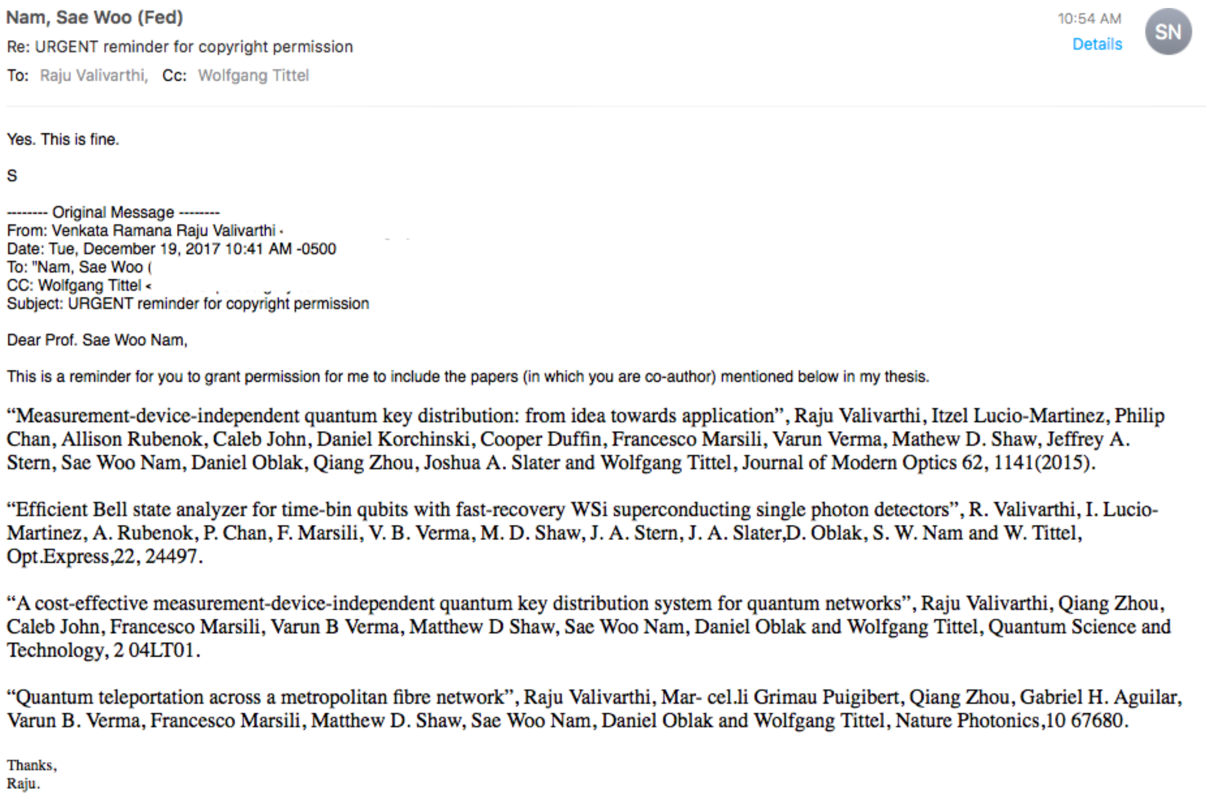
"Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors", R. Valivarthi, I. Lucio-Martinez, A. Rubenok, P. Chan, F. Marsili, V. B. Verma, M. D. Shaw, J. A. Stern, J. A. Slater,D. Oblak, S. W. Nam and W. Tittel, Opt.Express,22, 24497.

"A cost-effective measurement-device-independent quantum key distribution system for quantum networks", Raju Valivarthi, Qiang Zhou, Caleb John, Francesco Marsili, Varun B Verma, Matthew D Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Quantum Science and Technology, 2 04LT01.

"Quantum teleportation across a metropolitan fibre network", Raju Valivarthi, Mar- cel.li Grimau Puigibert, Qiang Zhou, Gabriel H. Aguilar, Varun B. Verma, Francesco Marsili, Matthew D. Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Nature Photonics,10 67680.

Thank you,
Raju.

Figure F.14: Copyright permissions from Matthew Shaw.



Nam, Sae Woo (Fed)
Re: URGENT reminder for copyright permission
To: Raju Valivarthi, Cc: Wolfgang Tittel

Yes. This is fine.

S

-------- Original Message --------
From: Venkata Ramana Raju Valivarthi ·
Date: Tue, December 19, 2017 10:41 AM -0500
To: "Nam, Sae Woo (
CC: Wolfgang Tittel <
Subject: URGENT reminder for copyright permission

Dear Prof. Sae Woo Nam,

This is a reminder for you to grant permission for me to include the papers (in which you are co-author) mentioned below in my thesis.

“Measurement-device-independent quantum key distribution: from idea towards application”, Raju Valivarthi, Itzel Lucio-Martinez, Philip Chan, Allison Rubenok, Caleb John, Daniel Korchinski, Cooper Duffin, Francesco Marsili, Varun Verma, Mathew D. Shaw, Jeffrey A. Stern, Sae Woo Nam, Daniel Oblak, Qiang Zhou, Joshua A. Slater and Wolfgang Tittel, Journal of Modern Optics 62, 1141(2015).

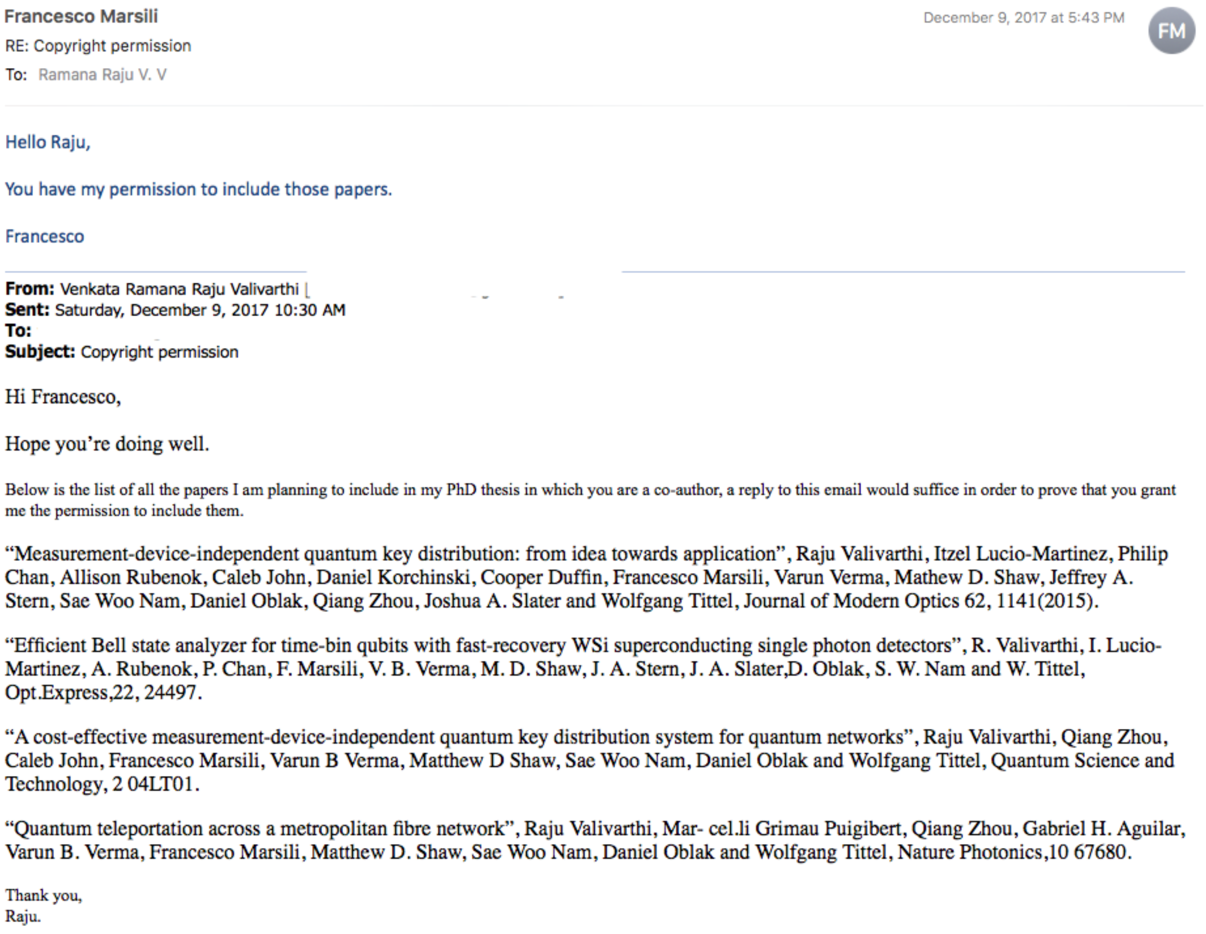
“Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors”, R. Valivarthi, I. Lucio-Martinez, A. Rubenok, P. Chan, F. Marsili, V. B. Verma, M. D. Shaw, J. A. Stern, J. A. Slater,D. Oblak, S. W. Nam and W. Tittel, Opt.Express,22, 24497.

“A cost-effective measurement-device-independent quantum key distribution system for quantum networks”, Raju Valivarthi, Qiang Zhou, Caleb John, Francesco Marsili, Varun B Verma, Matthew D Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Quantum Science and Technology, 2 04LT01.

“Quantum teleportation across a metropolitan fibre network”, Raju Valivarthi, Mar- cel.li Grimau Puigibert, Qiang Zhou, Gabriel H. Aguilar, Varun B. Verma, Francesco Marsili, Matthew D. Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Nature Photonics,10 67680.

Thanks,
Raju.

Figure F.15: Copyright permissions from Sae-Woo Nam.



Francesco Marsili

RE: Copyright permission

To: Ramana Raju V. V

December 9, 2017 at 5:43 PM

FM

Hello Raju,

You have my permission to include those papers.

Francesco

From: Venkata Ramana Raju Valivarthi [
Sent: Saturday, December 9, 2017 10:30 AM
To:
Subject: Copyright permission

Hi Francesco,

Hope you're doing well.

Below is the list of all the papers I am planning to include in my PhD thesis in which you are a co-author, a reply to this email would suffice in order to prove that you grant me the permission to include them.

"Measurement-device-independent quantum key distribution: from idea towards application", Raju Valivarthi, Itzel Lucio-Martinez, Philip Chan, Allison Rubenok, Caleb John, Daniel Korchinski, Cooper Duffin, Francesco Marsili, Varun Verma, Mathew D. Shaw, Jeffrey A. Stern, Sae Woo Nam, Daniel Oblak, Qiang Zhou, Joshua A. Slater and Wolfgang Tittel, Journal of Modern Optics 62, 1141(2015).

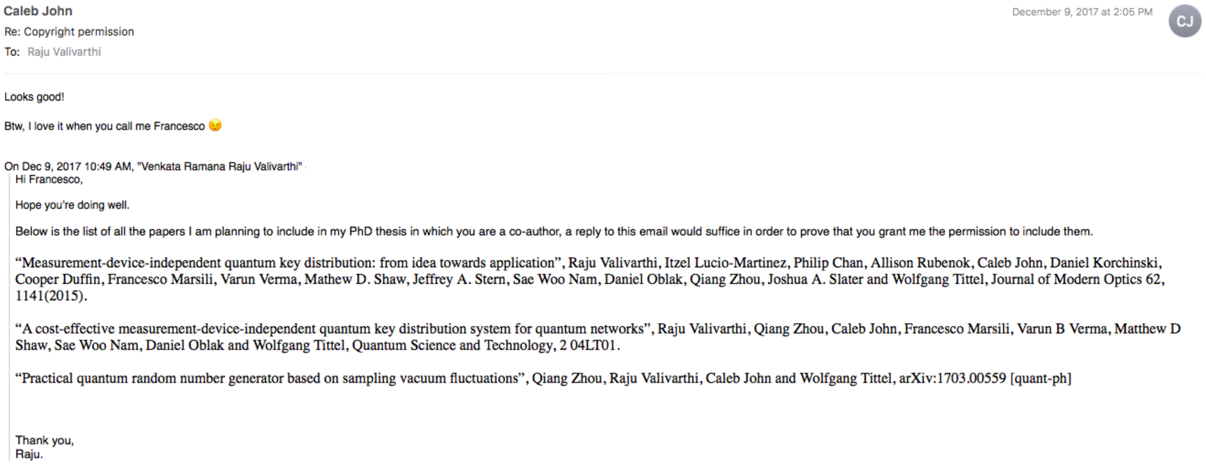
"Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors", R. Valivarthi, I. Lucio-Martinez, A. Rubenok, P. Chan, F. Marsili, V. B. Verma, M. D. Shaw, J. A. Stern, J. A. Slater,D. Oblak, S. W. Nam and W. Tittel, Opt.Express,22, 24497.

"A cost-effective measurement-device-independent quantum key distribution system for quantum networks", Raju Valivarthi, Qiang Zhou, Caleb John, Francesco Marsili, Varun B Verma, Matthew D Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Quantum Science and Technology, 2 04LT01.

"Quantum teleportation across a metropolitan fibre network", Raju Valivarthi, Mar- cel.li Grimau Puigibert, Qiang Zhou, Gabriel H. Aguilar, Varun B. Verma, Francesco Marsili, Matthew D. Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Nature Photonics,10 67680.

Thank you,
Raju.

Figure F.16: Copyright permissions from Francesco Marsili.



Caleb John
Re: Copyright permission
To: Raju Valivarthi

December 9, 2017 at 2:05 PM

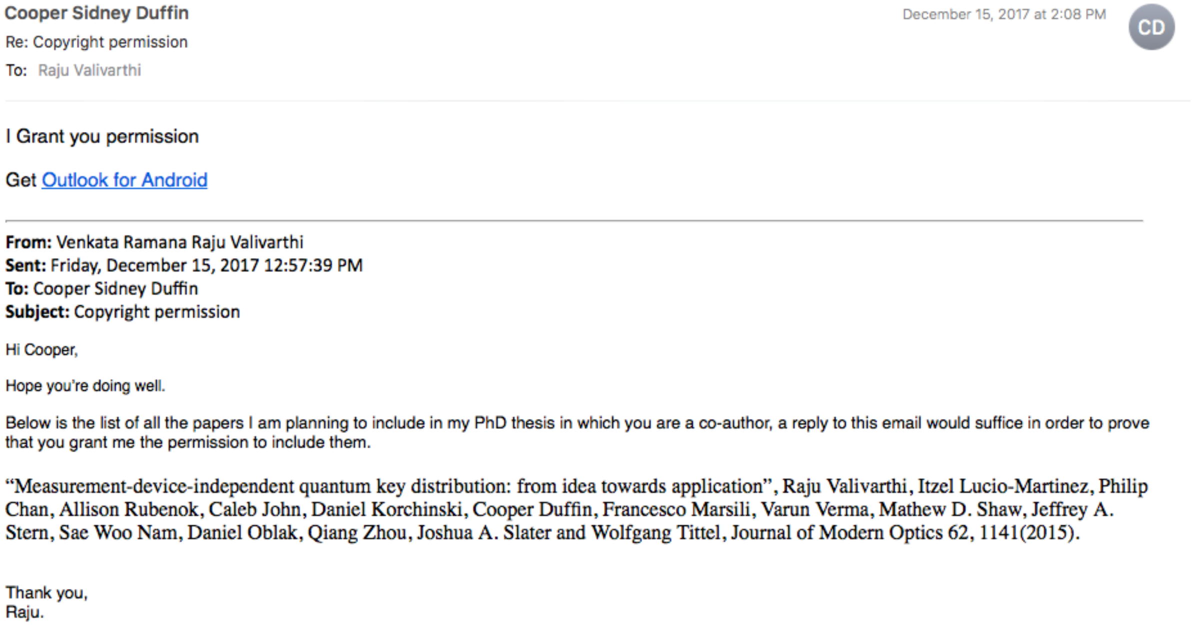
Looks good!

Btw, I love it when you call me Francesco 😉

On Dec 9, 2017 10:49 AM, "Venkata Ramana Raju Valivarthi"

> Hi Francesco,
>
> Hope you're doing well.
>
> Below is the list of all the papers I am planning to include in my PhD thesis in which you are a co-author, a reply to this email would suffice in order to prove that you grant me the permission to include them.
>
> “Measurement-device-independent quantum key distribution: from idea towards application”, Raju Valivarthi, Itzel Lucio-Martinez, Philip Chan, Allison Rubenok, Caleb John, Daniel Korchinski, Cooper Duffin, Francesco Marsili, Varun Verma, Mathew D. Shaw, Jeffrey A. Stern, Sae Woo Nam, Daniel Oblak, Qiang Zhou, Joshua A. Slater and Wolfgang Tittel, Journal of Modern Optics 62, 1141(2015).
>
> “A cost-effective measurement-device-independent quantum key distribution system for quantum networks”, Raju Valivarthi, Qiang Zhou, Caleb John, Francesco Marsili, Varun B Verma, Matthew D Shaw, Sae Woo Nam, Daniel Oblak and Wolfgang Tittel, Quantum Science and Technology, 2 04LT01.
>
> “Practical quantum random number generator based on sampling vacuum fluctuations”, Qiang Zhou, Raju Valivarthi, Caleb John and Wolfgang Tittel, arXiv:1703.00559 [quant-ph]
>
> Thank you,
> Raju.

Figure F.17: Copyright permissions from Caleb John.



Cooper Sidney Duffin
Re: Copyright permission
To: Raju Valivarthi

December 15, 2017 at 2:08 PM

I Grant you permission

Get Outlook for Android

From: Venkata Ramana Raju Valivarthi
Sent: Friday, December 15, 2017 12:57:39 PM
To: Cooper Sidney Duffin
Subject: Copyright permission

Hi Cooper,

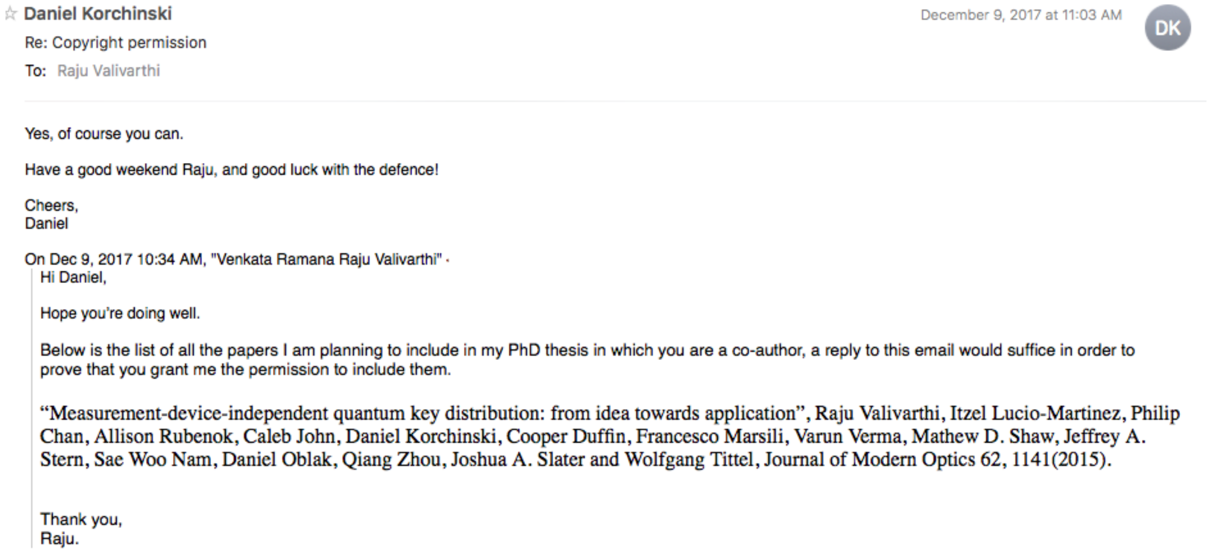
Hope you're doing well.

Below is the list of all the papers I am planning to include in my PhD thesis in which you are a co-author, a reply to this email would suffice in order to prove that you grant me the permission to include them.

“Measurement-device-independent quantum key distribution: from idea towards application”, Raju Valivarthi, Itzel Lucio-Martinez, Philip Chan, Allison Rubenok, Caleb John, Daniel Korchinski, Cooper Duffin, Francesco Marsili, Varun Verma, Mathew D. Shaw, Jeffrey A. Stern, Sae Woo Nam, Daniel Oblak, Qiang Zhou, Joshua A. Slater and Wolfgang Tittel, Journal of Modern Optics 62, 1141(2015).

Thank you,
Raju.

Figure F.18: Copyright permissions from Cooper Duffin.



☆ **Daniel Korchinski**

December 9, 2017 at 11:03 AM

DK

Re: Copyright permission

To: Raju Valivarthi

Yes, of course you can.

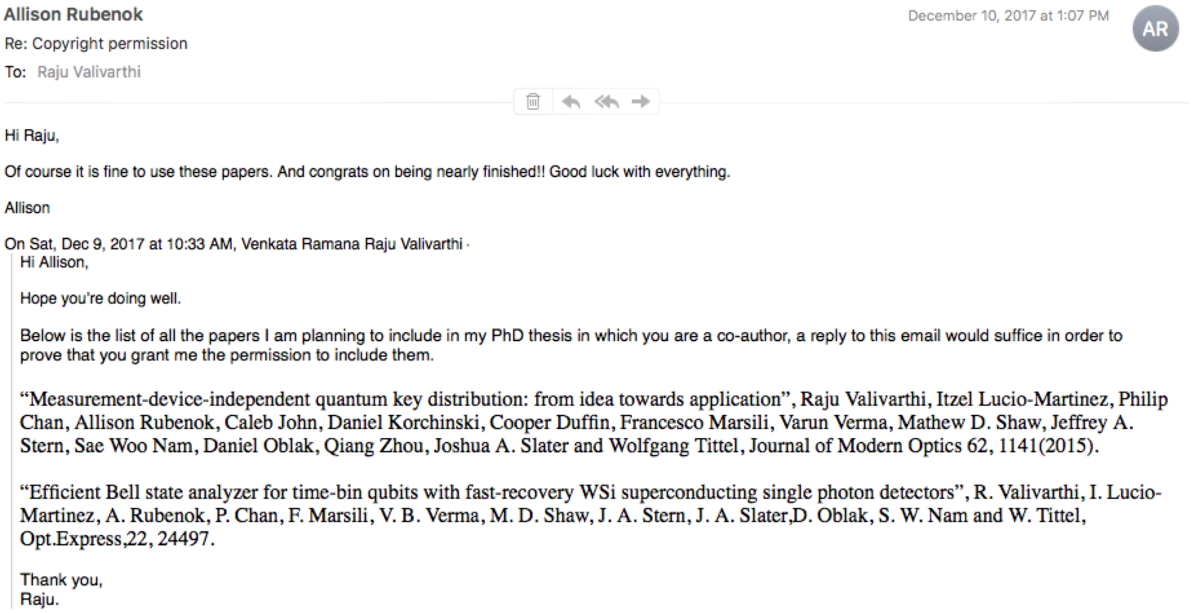
Have a good weekend Raju, and good luck with the defence!

Cheers,
Daniel

On Dec 9, 2017 10:34 AM, "Venkata Ramana Raju Valivarthi" ·

> Hi Daniel,
>
> Hope you're doing well.
>
> Below is the list of all the papers I am planning to include in my PhD thesis in which you are a co-author, a reply to this email would suffice in order to prove that you grant me the permission to include them.
>
> "Measurement-device-independent quantum key distribution: from idea towards application", Raju Valivarthi, Itzel Lucio-Martinez, Philip Chan, Allison Rubenok, Caleb John, Daniel Korchinski, Cooper Duffin, Francesco Marsili, Varun Verma, Mathew D. Shaw, Jeffrey A. Stern, Sae Woo Nam, Daniel Oblak, Qiang Zhou, Joshua A. Slater and Wolfgang Tittel, Journal of Modern Optics 62, 1141(2015).
>
> Thank you,
> Raju.

Figure F.19: Copyright permissions from Daniel Korchinski.



Allison Rubenok

December 10, 2017 at 1:07 PM

AR

Re: Copyright permission

To: Raju Valivarthi

Hi Raju,

Of course it is fine to use these papers. And congrats on being nearly finished!! Good luck with everything.

Allison

On Sat, Dec 9, 2017 at 10:33 AM, Venkata Ramana Raju Valivarthi ·

> Hi Allison,
>
> Hope you're doing well.
>
> Below is the list of all the papers I am planning to include in my PhD thesis in which you are a co-author, a reply to this email would suffice in order to prove that you grant me the permission to include them.
>
> "Measurement-device-independent quantum key distribution: from idea towards application", Raju Valivarthi, Itzel Lucio-Martinez, Philip Chan, Allison Rubenok, Caleb John, Daniel Korchinski, Cooper Duffin, Francesco Marsili, Varun Verma, Mathew D. Shaw, Jeffrey A. Stern, Sae Woo Nam, Daniel Oblak, Qiang Zhou, Joshua A. Slater and Wolfgang Tittel, Journal of Modern Optics 62, 1141(2015).
>
> "Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors", 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, Opt.Express,22, 24497.
>
> Thank you,
> Raju.

Figure F.20: Copyright permissions from Allison Rubenok.