UNIVERSITY OF CALGARY

Quantum Correlations for Fundamental Tests and Quantum Communication

by

Joshua A. Slater

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF PHYSICS AND ASTRONOMY

CALGARY, ALBERTA

MAY, 2013

UNIVERSITY OF CALGARY

FACULTY OF GRADUATE STUDIES

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies for acceptance, a thesis entitled "Quantum Correlations for Fundamental Tests and Quantum Communication" submitted by Joshua A. Slater in partial fulfillment of the requirements for the degree of DOCTOR OF PHILOSOPHY.

Dr. Wolfgang Tittel
Department of Physics and Astronomy,
University of Calgary

Dr. Anton Zeilinger
Austrian Academy of Sciences,
and
Faculty of Physics,
University of Vienna

Dr. Alex Lvovsky
Department of Physics and Astronomy,
University of Calgary

Dr. Jorgen S. Nielsen
Department of Electrical and Computer Engineering,
University of Calgary

Dr. Paul Barclay
Department of Physics and Astronomy,
University of Calgary

Date

Abstract

Quantum correlations arising from measurements on pairs of entangled particles are often referred to as the most non-classical feature of quantum mechanics. As such, they have found a role in many fundamental tests of quantum mechanics and most emerging applications in the field of quantum communication. The most well-known fundamental test is the Bell inequality. Its repeated violation in countless experiments has convinced physicists that local hidden variables cannot describe the correlations arising from measurements on entangled particles. On the application side, quantum correlations have been used in quantum key distribution, which aims to provably secure messages during transmission, and quantum repeaters, which are essential for future long-distance quantum communication.

The main goal of this thesis was to use quantum entanglement for new fundamental studies and quantum communication applications. Towards this end, we developed a high-fidelity source of entanglement and used it in a fundamental test where we bounded the predictive power any physical theory could have about the outcomes of measurements on entangled particles. Secondly, we made use of entangling measurements to develop a new quantum cryptography system based on the promising MDI-QKD protocol, which protects users from otherwise undetectable hacking attacks. We developed a detailed model of MDI-QKD systems with which one can optimize any implementation, deployed our MDI-QKD system across the city of Calgary, and demonstrated the feasibility of this protocol and of long-distance entangling measurements. Thirdly, we have built a source of entanglement compatible with quantum memories, which is an essential ingredient of quantum repeaters. We then demonstrated several crucial steps towards a functioning quantum repeater, including the preservation of entanglement during storage and, more generally, the entire photonic wavefunction. While further work is required to bring our demonstrations to real-world applications, we are confident that they will prove useful in guiding future developments.

List of published and submitted articles in this thesis

Articles are listed in the order they appear in this thesis. Supplemental Materials and Supplementary Information contained in the appendix at the end of the thesis.

3.1 T. E. Stuart, J. A. Slater, F. Bussières, W. Tittel, A flexible source of non-degenerate entangled photons based on a two-crystal Sagnac interferometer, arXiv:1305.0986, 5 May 2013.

3.2 T. E. Stuart, J. A. Slater, R. Colbeck, R. Renner and W. Tittel, An experimental test of all theories with predictive power beyond quantum theory, *Physical Review Letters* **109** (2): 020402, 9 July 2012.

4.1 P. Chan, J. A. Slater, P. Chan, I. Lucio-Martinez, A. Rubenok and W. Tittel, Modeling a Measurement-Device-Independent Quantum Key Distribution System, arXiv.org:1204.0738, 3 April 2012.

4.2 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, arXiv.org:1304.2463, 9 April 2013.

5.1 E. Saglamyurek, N. Sinclair, J. Jin, J. A. Slater, D. Oblak, F. Bussières, M. George, R. Ricken, W. Sohler and W. Tittel, Conditional detection of pure quantum states of light after storage in a Tm-doped waveguide, *Physical Review Letters* **108** (8): 083602, 22 February 2012.

5.2 J. Jin, J. A. Slater, E. Saglamyurek, N. 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, arXiv.org:1302.2177, 8 February 2013.

5.3 E. Saglamyurek, N. Sinclair, J. Jin, J. A. Slater, D. Oblak, F. Bussières, M. George, R. Ricken, W. Sohler and W. Tittel, Broadband waveguide quantum memory for entangled photons, *Nature* **469** (7331): 512 - 515, 12 January 2011.

Acknowledgements

My Ph.D. would have been very different without the help of many individuals, all of whom deserve much thanks. First are the many past and present members of my research group, especially everyone who has spent so many long hours with me in our often dark labs: Allison Rubenok, Philip Chan, Erhan Saglamyurek, Terence Stuart, Itzel Lucio Martinez, Jeongwan Jin, and Neil Sinclair. I hope we continue to find a way to work together. I further thanks to Philip, Erhan, Félix Bussières and Morgan Hedges for so many interesting and useful discussions over the years, it has always been, and hopefully will continue to be, a pleasure to turn to you to talk. I thank Vladimir Kiselyov and Steve Hosier for their support, and I hope you realize how invaluable your expertise has been. I thank Daniel Oblak and Hassan Mallahzadeh for keeping the memory lab a lively place as well as Daniel Korchinski, Mike Lamont and Yang Tan for the fun, but sadly-too-brief, work together. Lastly, I want to thank those who helped shape this incredible group in the early days, but have moved on long ago, Chris Healey, Cecilia La Mela, Xiaofan Mo, Aida Delfan and Gina Howard, as well as those just starting who are clearly keeping the fun and excitement alive, Marcel-li Grimau Puigibert, Raju Valivarthi, Thomas Lutz and Lambert Giner.

I want to thank my many external collaborators who all made significant contributions to the work here. Special thanks is deserved for the e-mail support that Roger Colbeck, Jean-Daniel Bancal, Nicolas Brunner, Cyril Branciard and Renato Renner have given me long after our papers were published. Whether it was Bell inequalities or security proofs that had completely confused me, their thoughtful e-mails always got me straight again.

Many thanks go to all the members of PHAS from the past five years, especially Christoph Simon and Catherine Barrett, who have become both colleagues and friends. In many capacities Christoph has been a mentor and I thank him for his guidance and insightful perspectives in science, teaching and careers. And Catherine, for her tireless help on so

many levels, both professional and personal, on so many different tasks, and on so many problems. She's been our keeper-of-knowledge and our jack-of-all-non-lab-trades. Often the only sane person in this insane place, it's frightening to imagine being here without her. And also Tracy Korsgaard for her help navigating the endless bureaucracy of graduate school, Nancy Lu for all her help around IQST.

Perhaps most deservedly of my gratitude is my supervisor Wolfgang Tittel. I know that I've grown a lot under his tutelage and I must thank Wolfgang for inviting me to be part of the team, and for making this such a great environment. With his endless energy, insight, patience and other great qualities, Wolfgang has been more than a boss, but a leader, a teacher, and a colleague. Reminding myself that he's the 'chief' is at times tricky, because of the great relationship he's fostered. It has always been a real pleasure working with you.

Many people outside of the degree deserve much thanks. Jyotsna Kashyap for always being available to talk and encourage, Nicolas Choquette-Levi for listening to me rant and lending a hand with life when I couldn't get off work, Randy Squires for his constant amusement and introducing me to a great past-time, Orion Penner for forcing entertainment when it was most needed, Rob Rubenok for his wacky ideas and always being there in a pinch, Tim Friesen for his generosity and patience with my wacky ideas, and most importantly, my best friend, Allison Rubenok. Not only have we slaved together in the lab and over many papers, but we've adventured the world together. Thank you for your patience with me, for every sacrifice you made for me, and always being there to help in whatever way I needed

I must also thank my mom and dad, Barb and Kim, and my brother Peter. They have always supported me and encouraged me, even though they might not follow what I've been doing. Where ever you are, I know you're all very proud.

Table of Contents

List of Figures and Illustrations

List of Tables

List of Abbreviations

Abbreviation	Definition
AFC	Atomic Frequency Comb
AOM	Acousto-Optic Modulator
ATT	Attenuator
APD	Avalanche Photo Diode
BB84	Bennett, Brassard 1984
BS	Beamsplitter
BSC	Babinet-Soleil phase Compensator
BSM	Bell-State Measurement
CHSH	Clauser, Horne, Shimony, Holt
CCW	Counter-Clockwise
CLN	Congruent Lithium Niobate
CRIB	Controlled Reversible Inhomogeneous Broadening
CM	Classical Memory
CW	Clockwise
CW	Continuous Wave
DI-QKD	Device Independent QKD
DM	Dichroic Mirror
EIT	Electromagnetically Induced Transparency
EPR	Einstein, Podolsky & Rosen
FBG	Fibre Bragg Grating
FD	Frequency Doubler
FPF	Fabry-Perot Filter
FS	Frequency Shifter
FWHM	Full-Width Half Maximum
GEM	Gradient Echo Memory
HOM	Hong-Ou-Mandel
HWP	Half-Wave Plate
IM	Intensity Modulator
InGaAs	Indian Gallium Arsinide
LD	Laser Diode
LHV	Local Hidden Variables
$LiNbO_3$	Lithium Niobate
MC	Master Clock
MDI-QKD	Measurement Device Independent QKD
MEMS	Microelectromechanical system
NDF	Neutral Density Filter
PBS	Polarizing Beam Splitter
PC	Personal Computer
PC	Polarization Controller
PM	Phase Modulator
PNS	Photon Number Splitting

POC	Polarization Controller
PPLN	Periodically-Poled Lithium Niobate
QC2	Quantum Cryptography and Communication Labs
QED	Quantum Electrodynamics
QKD	Quantum Key Distribution
QM	Quantum Memory
QST	Quantum State Tomography
QWP	Quarter-Wave Plate
SAIT	Southern Alberta Institute of Technology Polytechnique
SFWM	Spontaneous Four-Wave Mixing
Si	Silicon
SNR	Signal-to-Noise Ratio
SPD	Single Photon Detector
SPDC	Spontaneous Parametric Down-Conversion
SV	Spacetime Variable
Ti:Tm:$LiNbO_3$	Titanium Thulium Lithium Niobate
Tm	Thulium
TM	Transverse Magnetic
TDC	Time-to-Digital Converter
UofC	University of Calgary

Chapter 1

Introduction

1.1 Quantum Entanglement

Quantum entanglement is commonly considered to be the most non-classical feature of quantum mechanics. Measurements on two entangled particles can show individually perfect randomness while simultaneously showing perfect correlation. The existence of such correlations begs for explanation, but should not, intuitively, appear surprising, as similar correlations appear everyday, all around us. A group of pedestrians at an intersection will cross the street at a random but simultaneous time. Their response is correlated because all receive a "walk signal" persuading them to walk at a specific time. As another example, when one observes the socks on university students one finds a random collection of colours, but matching colours on any one student's pair of feet (perfect correlation). In this case, the correlation upon inspection of the student's socks arrises because the student has decided beforehand that his socks should match - the colour of his socks has a pre-determined, well-defined value. The correlations around us are explainable with "signals" or pre-determined values, and this is in striking opposition to quantum mechanics. Correlations between entangled particles exist regardless of the distance between the particles and regardless of the time between the measurements, suggesting that a "signal" between the particles is not the explanation. Also, quantum mechanics says that particles cannot have a well-defined value for all possible measurements simultaneously (e.g. position and momentum), suggesting that the existence of pre-determined values is not the explanation. These correlations and quantum entanglement is where quantum mechanics departs from classical reasoning and as such, they are at the centre of fundamental tests of quantum mechanics as well as most applications of quantum information processing, including quantum communication.

The "spooky" properties of entanglement were first recognized by Einstein, Podolsky and Rosen [1] and Schrödingier, who coined the term entanglement [2], in 1935. EPR argued that the outcome of any measurement on any particle must be determined prior to the measurement and cannot depend on actions that are space-like separated. They agued that these two assumptions, known as realism and locality, must be obeyed in any physical description of reality. Such assumptions seem natural as they agree with every experience in classical physics and certainly our own personal experiences. EPR then argued that if entangled particles give rise to perfect correlations, than there must be an underlying *element of reality* that deterministically produced these outcomes. Today these elements are referred to as *local hidden variables* and, if they existed, would allow one to deterministically predict the outcome of every possible measurement. As deterministic predictions for every measurement disagrees with quantum mechanics, EPR concluded that quantum mechanics must be incomplete. It is important to note that EPR never argued that quantum mechanics was wrong, merely that it must be an incomplete theory and that another theory, which upheld local deterministic predictions, would supersede it.

It is not surprising that EPR used the most non-classical feature in their argument against quantum mechanics. Nevertheless, in many ways, EPR had created a challenge for physicists. Either entanglement, and thus, quantum mechanics must be replaced by a more powerful theory or the widely-believed notion of local realism does not apply in general – an important fundamental question.

The issue remained largely philosophical until the early 1960s. At that point the Irish physicist John Steward Bell took up the challenge of developing a theory in the vision of EPR [3]. He accepted the EPR view and his starting point was that quantum physics was incomplete and that local realism must be upheld. However, after much effort, Bell was unable to construct a theory based on local hidden variables that reproduced all the measurement statistics of entangled particles. In fact, Bell proved just the opposite. He

developed mathematical constraints on the local-realistic correlations between measurement outcomes of two-particle systems and, moreover, demonstrated that correlations stemming from entangled particles violate those constraints. These constraints, known as *Bell inequalities*, showed that the quantum entanglement could not be reconciled with classical locality and realism.

An important feature of Bell's work is that his inequalities led to experimental tests. It was possible to experimentally test the difference between local realism and quantum entanglement, as will be discussed in the next section. Furthermore, as we will see in the following sections, the growing ability to harness this new phenomenon led to new quantum applications. Some examples are: quantum cryptography [4, 5, 6, 7], which will be discussed in section 1.3, quantum teleportation [8] and entanglement swapping [9], which will be discussed in conjunction with quantum repeaters in section 1.4, and quantum computing [10, 11].

1.2 Quantum Entanglement for Fundamental Tests

To test whether quantum mechanics is correct and whether entanglement, and hence nonlocality, exists, one must turn to experimentation. Answering this question has relied on searching for experimental violations of Bell inequalities. In this section I restrict the discussion to experimental tests of entanglement and begin with the most famous Bell inequality, known as the CHSH inequality [12], which is named after its inventors, Clauser, Horne, Shimony and Holt.

In this experiment, consider a pair of particles with each particle of the pair delivered to one of two physicists at very distant measuring stations. Each physicist, commonly named Alice and Bob, has a measurement device that takes as input a binary value specifying one of two measurements that each physicist will perform on their particle. Each measurement device can output only one of two answers: $+1$ or -1 (see Fig. 1.1). We call the two

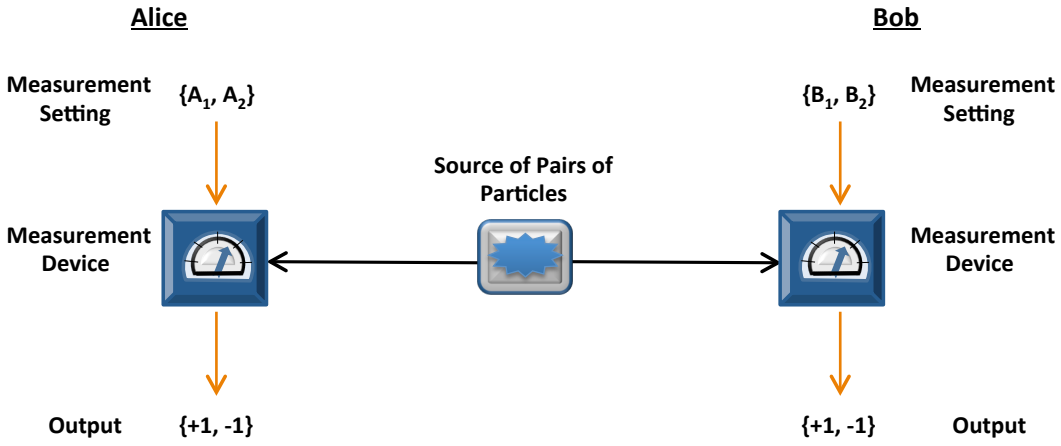


Figure 1.1: Bell inequality scenario. A source of pairs of particles distributes one particle to Alice and one particle to Bob. Alice chooses between two measurement settings (e.g. inputs) for her measurement device $\{A_1, A_2\}$ and receives one of two outputs $\{+1, -1\}$. Similarly for Bob.

measurement settings for Alice A_1 and A_2 and the two measurement settings B_1 and B_2 for Bob. For each pair of particles, Alice and Bob randomly, and individually, decide which of their measurements to perform, and record the output as a^m or b^n, where the superscript indicates the measurement setting. This is repeated for a large number of pairs, N, where the measurement results of the i^{th} pair is recorded as a_i^m and b_i^n. Afterwards, Alice and Bob come together and, for each pair of particles, they then calculate the product of their individual results and then find the average for all pairs measured with the same measurement settings. This is known as a correlation coefficient and is easily calculable: $E(A_m, B_n) = \sum_i a_i^m b_i^n / N$. If the four correlation coefficients could stem from an underlying local hidden variable, then it can be shown that the following is true:

$$S = |E(A_1, B_1) + E(A_1, B_2) + E(A_2, B_1) - E(A_2, B_2)| \leq 2 \tag{1.1}$$

This is the CHSH inequality, and S is known as the *Bell parameter*. Most importantly, the scenario described above as well as the derivation do not rely on quantum mechanics and is applicable to any physical system.

Experimental tests of the CHSH inequality rely on particle measurement with two possible answers. Henceforth, we will refer to these particles as *qubits*. For quantum mechanics, interestingly, the situation where the CHSH inequality is maximally violated is not when correlations are maximal but instead when the correlation coefficients $E(A_1, B_1) = E(A_1, B_2) = E(A_2, B_1) = -E(A_2, B_2) = 1/\sqrt{2}$, resulting in an S parameter of $2\sqrt{2}$.

The first tests of Bell inequalities were performed in 1972 by Stuart Freedman and John Clauser [13] and did produce a violation (i.e. $S > 2$). This was followed by the more famous, and more convincing, experiments by Alain Aspect *et al.* between 1981 and 1982 [14, 15, 16], who also observed a violation. Since then, many experimental tests (see [17, 18, 19, 20, 21, 22, 23] for notable experiments) have confirmed the quantum prediction - correlations unexplainable by local hidden variables.

While countless experiments to date have violated the Bell inequality, in every experiment there remains at least one potential "loophole" that could invalidate the conclusion and allow for a local hidden variable description. One of the most prominent loopholes is the locality loophole. In most experiments the correlations could be described by a slower-than-light (hence local) signal between the qubits or measurement devices that informs the qubits of the measurement settings at both measurement stations. Knowing the upcoming measurement settings the qubits could conspire to violate the Bell inequality. To close this loophole, the choice of measurement setting and the measurement itself at each measurement station must be space-like separated. Based on early locality-loophole work by Aspect *et al.* [16], the first experiment to fully close the locality loophole was Weihs *et al.* in 1998 [19]. A second loophole is known as the detection loophole. Given that most Bell experiments are performed with inefficient detectors and that qubits can be lost in apparata, it is possible that the detected qubits are the ones that give statistics that violate the Bell inequality, while the non-detected qubits would not. For the CHSH inequality with pure quantum states (see Chapter 2) an overall efficiency of 82.8% is needed to close this loophole, but this can be

lowered for non-maximally entangled states to 66.7% using Eberhard's inequality [24]. The first experiment to close the detection loophole was Rowe *et al.* in 2001 using atoms in an atomic trap [20]. Closing the detection loophole with photons was first achieved in 2013 by Giustina *et al.* [23]. The final loophole is known as the free choice loophole. Should the qubits under test have control of the measurements being performed they could easily violate a Bell inequality with local hidden variables. Closing this loophole with photons was first achieved by Scheidl *et al.* in 2010 [22].

While not all loopholes have been closed simultaneously, they have all been closed individually. Interest in Bell experiments continues today with a goal being a completely loophole-free test of a Bell inequality. Other fundamental motives to continue Bell tests exist as well. Quantum mechanics says that the correlations should exist over any distance, but could there be a distance limit? This was first tested by Tittel *et al.* in 1998 [18] with a Bell test over 10 km and more recently by Ursin *et al.* in 2007 [21] up to 144 km. Another fundamental question is whether a size or mass limits could exist. So far, Bell tests have been preformed with photons and electronic states in atoms. Quantum interference has also been observed with molecules as large as carbon-60 bucky balls (containing 720 nucleons!) [25]. Observing quantum effects with nano-mechanical objects is also in progress [26].

Moreover, while physicists are largely convinced that local hidden variables are not compatible with the predictions of quantum mechanics (and believe that a loophole-free Bell test will soon confirm this), some physicists have began to consider the existence of non-local hidden variables. The first series of tests of a specific non-local hidden variable theory began in 2007 [27, 28, 29]. More recently, we have experimentally worked on excluding general non-local variables theories (see Chapter 3).

Finally, Bell tests have applications in testing quantum devices and quantum communication channels. The simplest way to test that a novel source of entangled particles actually generates entanglement is to observe a Bell violation (see Chapter 3). Testing whether a

device, such as a quantum communication channel (see Chapter 4) or a quantum memory (see Chapter 5), can preserve quantum entanglement, is also easily done by observing a Bell violation

1.3 Quantum Entanglement for Quantum Cryptography

One goal of cryptography is to provide secure and confidential communication between two distant parties. If two parties share a key (i.e. a string of ones and zeros), of which no one else has knowledge, than this *secret* key can be used for secure encryption and transmission of messages by use of the *one-time pad* algorithm. This algorithm cannot be broken even in principle, but requires that the key be as long as the message itself and, most importantly, that the secret key is only used once. Therefore, to use a one-time pad the two parties require a technique to securely distribute secret keys. Due to this problem, most cryptographic systems today use other techniques for confidential communication that do not require the distribution of secret keys, but also cannot be proved secure, even in principle. Their security is based on computationally difficult problems that take enormous amounts of computational time to crack on conventional computers. However, its been proven that a quantum computer can efficiently crack some of these techniques. Regardless, given enough computation time, these techniques can always be broken. As such, a secure method of key distribution is desirable. Quantum Key Distribution (QKD), the most advanced application within quantum cryptography, provides a solution to this problem [6, 7]. QKD is the most advanced application in the field of quantum communication. It has led to the development of commercial systems [30], systems functioning over more than 100 km of fibre [31] and air [32] as well as networks [33, 34].

QKD was first discovered by Charles Bennett and Gilles Brassard in 1984 [4] and again independently discovered in 1991 by Arthur Ekert [5]. The general setting of key distribution involves two parties, Alice and Bob, separated by some distance. Connecting these parties is

a communication channel. In classical cryptography this channel allows for the exchange of classical information while for QKD, Alice and Bob are allowed to posses a quantum channel that allows for the exchange of qubits or quantum information. Furthermore, it is assumed that Alice's and Bob's labs are secured, but that an eavesdropper, known as Eve, could listen to or perform any operation on any signals in both the classical and quantum channels (see Appendix A.2 for a detailed discussion of the assumptions for secure key distribution). The goal for Alice and Bob is to guarantee the distribution of a secret key of which Eve has no knowledge.

Here we will briefly outline the protocol introduced by Ekert. A source of two-qubit entanglement sends one qubit to Alice and one qubit to Bob. Each party again has a measurement device with three settings (e.g. labelled A_1, A_2, A_3 and B_1, B_2, B_3) such that one pair of settings (say A_1 and B_1) will generate perfectly correlated results (perfectly correlated strings of ones and zeros) and the remaining settings (A_2, A_3 and B_2, B_3) are used to test a Bell inequality. As above, Alice and Bob randomly and independently choose a measurement setting for their qubit of each pair and after a large number of pairs has been measured, they publicly reveal their measurement settings for each qubit (known as *basis reconciliation*). Results where Alice and Bob both chose the first setting are kept secret and will be used to form the secret key. Results where Alice and Bob both chose from the remaining settings are used to verify the security of that key through a Bell test. As Eve's goal is to gain knowledge of the bits in the secret key and therefore she would have to learn the results of Alice's and Bob's measurements. However, if Eve had done anything to the qubits during transmission that gave her information about the results of Alice's and Bob's measurements, then her knowledge constitutes a local hidden variable, and thus Alice and Bob will not violate the Bell inequality. Eve's attempt to gain information breaks the entanglement between Alice and Bob, and this will be detected.

In theory, the results from A_1 and B_1 are perfectly correlated and the Bell inequality

is maximally violated, however in a real implementation there are errors. In general, any deviation from perfect correlation (or non-maximal Bell violation) is assumed to be caused by an eavesdropper gaining partial information for the key. If the correlation between Alice's and Bob's results are high enough, they can use standard error correction techniques [35] to create a perfectly correlated key and standard privacy amplification [36] to remove any partial information Eve might have about that key. The most important feature is that by assessing error probabilities and the Bell violation, Alice and Bob can prove the security of the key before using it for message transmission with a one-time pad. This level of verification is not possible with any classical cryptography.

An important point on security is that QKD does not need to rely on the violation of a Bell inequality. There exists protocols that use entanglement but whose security relies on strong correlations for multiple measurement settings, such as [37]. Additionally, QKD does not even need to rely on entanglement. In fact, in many protocols, including the original BB84, Alice prepares the quantum state of a single qubit, which she sends to Bob to measure. These protocols, known as prepare-and-measure protocols, are also provably secure. Their security can be argued by appealing to two principles. First, security against attacks based on individual particle operations can be argued by appealing to the *no-cloning* theorem of quantum mechanics [38]. Eve cannot create a perfect copy of the quantum state sent to Bob without necessarily changing the original state. This change leads to errors that alerts Alice and Bob to Eve's presence. More generally, attacks based on a coherent operation between many particles can be argued based on the fact that any measurement Eve uses to extract information about their quantum states disturbs those quantum states and, again, introduces errors [7]. Given that security can be proven without relying on the more complicated sources of entanglement, commercial systems and most highly-developed research systems use prepare-and-measure schemes.

Nevertheless, entanglement has an important role in QKD. The security discussed so far

assumes that Eve attacks the quantum signals during transmission and that all devices inside the laboratories of Alice and Bob function exactly according to theory. The latter is seldom true and any device functioning that deviates from theory could open a *side-channel* that Eve can attack (see Appendix A.2). For example, in prepare-and-measure protocols, if Alice accidentally prepares multiple qubits with the same quantum state, this opens the possibility for an attack known as photon (or particle) number splitting (PNS) [39]. Eve can keep and measure one of the particles (after basis reconciliation) while ensuring that the remaining particles reach Bob, thus gaining information without introducing errors. This is an example of a broader class of side-channels based on Alice unintentionally leaking information of her prepared quantum state into other degrees of freedom [40]. Furthermore, as Alice's and Bob's labs allow for the transfer of qubits, it may be possible for Eve to send her own signals (classical or quantum) into these laboratories, which could allow for passive monitoring or even active controlling of devices. For example, in another experimentally demonstrated series of attacks, known as detector blinding [41], Eve sends light into Bob's laboratory to gain active control of his detectors. Eve then measures every particle Alice prepares, sends another signal to Bob and then only allows Bob's detectors to register a detection if there will be no errors. Again, Eve gains information without producing errors. Other known side-channel attacks include the time-shift attack [42] and the trojan horse attack [43].

While these side-channel attacks have counter-measures (for example, decoy states to combat PNS attacks [44, 45, 46], new detector designs to combat blinding, etc.) that allow for secure QKD when properly implemented, the use of entanglement-based techniques is the only provable way to eliminate other, as of yet unknown, side-channel attacks. For example, in entanglement-based protocols like Ekert's, the source of entanglement could reside in Alice's lab where she could confirm that it does generate entanglement. Thus, side-channels involving the source leaking information to the environment (i.e. PNS attacks) would be detectable as this would constitute the existence of a hidden variable. In view

of detector blinding, a newer result is the ability to secure the measurement devices "with entanglement" [47, 48]. Rather than directly measuring the qubit he receives, Bob (or even someone else) could instead perform an entangling measurement (using a more sophisticated measurement device described in Chapter 2) with the qubit from Alice and a qubit of his own to create entanglement between him and Alice. If Eve controls this measurement device and tries any measurement other than an entangling measurement, she effectively breaks the entanglement between Alice and Bob, resulting in detectable errors.

Finally, there is active research into protocols known as *device-independent QKD* (DI-QKD), where the security of QKD can be proved solely on a Bell violation [7]. These DI-QKD protocols [49, 50] require no assumptions about the internal workings of Alice's and Bob's devices, but generally rely on a loophole free Bell tests between Alice's and Bob's labs. A loophole free Bell test ensures the security of Alice's source of entanglement, Bob's measurement device, and the channel in between. However, as a loophole free Bell test has not yet been performed, the practicality of these techniques in the near term is questionable. More recently, a more practical DI-QKD protocol was proposed that involves local loophole free Bell tests at Alice's and Bob's labs, as well as an entangling measurement between them [51].

1.4 Quantum Entanglement for Quantum Repeaters

The distribution of entanglement over long distances is essential for the future of quantum communication. QKD , communication between distance future quantum computers as well as long-distance fundamental tests all require long distance entanglement distribution. However, any quantum channel will be affected by loss, which limits the distance over which qubits can be sent. The same problem exists in classical telecommunications. Today, optical fibres can have an impressively low attenuation of 0.2 dB/km, which means that an optical signal's intensity drops by 50% after 15 km (compare this to standing in front of a 15-

km thick glass window. You would see absolutely nothing from the other side). However, after 100 km, only 1% of the signal remains, one ten-thousandths after 200 km, and one part in ten billion after 500 km. Imagine a single photon traveling the same distance. After 500 km (the driving distance between Vienna Austria and Nuremberg Germany, or between Calgary and Jasper Alberta) the probability that the photon makes the journey is 10^{-10}. Clearly, this exponential loss quickly makes *direct* communication, both classical and quantum, unworkable.

The problem is solved in classical telecommunications by repeater stations placed roughly every 100 kms. These repeaters amplify the remaining optical signal back to the original intensity. Essentially, they make many copies of the existing, classical, optical signal. Unfortunately, due to the quantum no-cloning theorem, this straightforward solution is not possible for single photons carrying quantum information. Instead, two solutions are being investigated. The first is to go free-space with satellite communication [52], and take advantage of the fact that absorption in air decreases with altitude. The main challenges of this approach are mostly technical, including issues such as optical tracking. The second approach, is to go with fibre optics and design a *quantum repeater*.

The quantum repeater was introduced by Briegel *et al.* in 1999 [53] as an efficient way to generate entanglement across long distance [54]. The idea is to start with a long channel and separate this channel into smaller *elementary links*. The actual number of elementary links depends on the length of the channel and the efficiency of the following steps. Next, one generates entanglement between the end points of each elementary link via direct transmission. For example, a source of entangled particles may sit in the middle of an elementary link and send one particle to each end point. Then, after all the end points of all the elementary links have shared entangled particles, each end point can perform *entanglement swapping* [9]: imagine that two qubits, A and B, are entangled with each other and another two qubits, C and D, are also entangled with each other. By performing an entangling measurement on

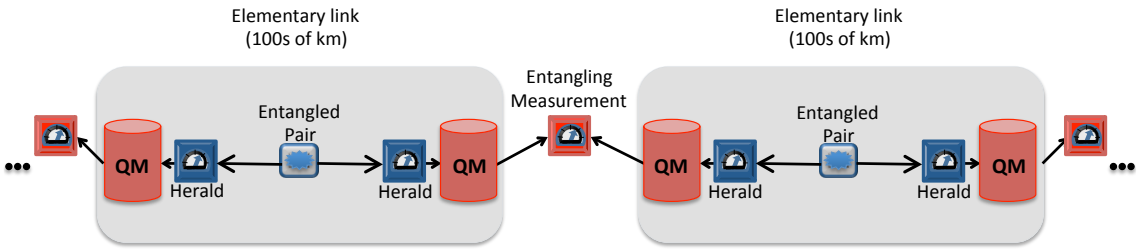


Figure 1.2: Quantum Repeater. As described in the text, entanglement is distributed across an elementary link spanning on the order of 100s of kms. Qubits are heralded before being stored in quantum memories (QM). Once two neighbouring elementary links have established entanglement between both of their respective end points, qubits are recalled from memories and an entangling measurement is performed to swap the entanglement. The ellipses represent that this procedure can be chained repeatedly.

qubits B and C (i.e. one qubit from each initial pair) the other two qubits, A and D, will become entangled. In the quantum repeater scenario, at the intersection of two elementary links are two end points (photons B and C). By performing entanglement swapping the far ends of these two elementary links (A and D) become entangled (see Fig. 1.2). Finally, entanglement swapping can be repeated, or chained, until entanglement is established between the ends of the original channel.

Two important requirements arise at this point [54]. First is that the initial entanglement distribution across each elementary link must be done in a *heralded* fashion. It must be known that the end points of an elementary link actually share entanglement. Second, as transmission across each elementary link will be probabilistic, each end point must store their entanglement until entanglement is created across the neighbouring elementary link, as only then is entanglement swapping possible. This necessitates *quantum memories*. Without quantum memories [55] to store these qubits, all transmissions would have to succeed simultaneously and there would be no advantage over direct transmission across the entire channel.

In the above architecture, quantum memories are devices that need to store qubits for an initially undetermined amount of time and then release them on demand. This combination

of heralding and on-demand recall from quantum memories essentially transforms probabilistic entanglement generation into entanglement generation on-demand, which is useful in other applications such as quantum computing.

Experimental investigation into quantum memory is extremely active and encompasses research into different systems and different materials [56] and different mechanisms to achieve faithful storage and recall [56, 57]. For quantum repeaters to function efficiently, memories require many features beyond recall-on-demand, including high-efficiency storage over long durations (this time is, in the best case, on the order of the communication time across an elementary link). For ease-of-use, they should be able to store short pulses and many qubits simultaneously. And they need to store qubits with high fidelity, preserve entanglement, and ensure that qubits remain suitable for entanglement swapping. In Chapter 5 I will discuss our work on verifying high-fidelity storage of a particular quantum memory, which will include demonstrations of entangling measurements required for entanglement swapping and the preservation of entanglement after storage.

The architecture presented above is just one example of a quantum repeater. There exist many variations on each component [58, 59, 60], including different types of memories (i.e. quantum memories that do not store incoming qubits, but generate two entangled qubits, each at a different time), different techniques for entanglement generation across elementary links [54], architectures allowing multimode storage [58] and shuffling between modes [60] etc. Most variations are more efficient than the architecture described above, but the advantage over direction transmission is clear. With quantum repeaters one does not need a single qubit to successfully travel all elementary links. Instead, qubits travel smaller elementary links and individual successes can be stored and built upon to achieve efficient long-distance quantum communication.

1.5 This Thesis

As discussed in this chapter, quantum communication can provide improvements over what can be achieved with classical communication techniques. In particular, the tremendous amounts of sensitive information that are now transmitted over public channels and secured by possibly breakable cryptography techniques could be protected by QKD, which is the only proven technique for verifiable, unconditional security. While small-scale and point-to-point QKD systems exist, it will take new technologies such as quantum repeaters to break the distance barrier and bring efficient quantum communication to truly long distances.

Perhaps not surprisingly, these technologies all rely on the most non-classical manifestation in quantum mechanics: quantum entanglement. The motivation for this thesis was to study the phenomenon of entanglement from novel perspectives and to make use of it in quantum communication applications. It covers research on new fundamental experiments on quantum non-local correlations and analyzes these correlations in the context of general non-local hidden variable models. On the applied side, techniques were developed that are applicable to both quantum cryptography and quantum repeater experiments. More specifically, this thesis contains the first experimental demonstration of a new approach to QKD, known as Measurement-Device Independent QKD (MDI-QKD). Our demonstration involves the first demonstration of a long-distance entangling measurement between photons from independent sources, which is also a key component of quantum repeaters. Furthermore, this thesis also shows the first entangling measurement between photons stored in independent quantum memories and the first demonstration of the storage and recall of an entangled photon from a solid-state device, both important pieces of future quantum repeaters.

This thesis is organized into six chapters. Chapter 1 covered an introduction to the topic. Chapter 2 will cover the basic elements (qubits, and measurements) required to understand following chapters. Chapter 3 will cover fundamental tests of quantum mechanics including a general approach to alternative non-local theories. Chapter 4 will cover the experimental

demonstration MDI-QKD, including a detailed theoretical model of the experiment and control systems for real-world entangling measurements. Chapter 5 will cover experimental demonstrations with quantum memories, which include entanglement storage and entangling measurements between photons stored in independent memories. The final chapter, Chapter 6, will draw some conclusions and discuss future work in these directions.

Chapters 3, 4 and 5 contain multiple articles and thus there is some topical overlap within and between these chapters. The supplementary information or supplemental materials for these papers appear as appendices at the end of this thesis.

This work would not have been possible without collaborations with several other individuals. As a member of the Quantum Cryptography and Communication (QC2) Labs' Entanglement team I have worked closely with many current and former members of my team: Jeongwan Jin, Allison Rubenok, Terence Stuart, and Dr. Félix Bussières. I have also been fortunate to closely collaborate with members of other QC2 teams, including the Memory team: Neil Sinclair, Dr. Erhan Saglamyurek and Dr. Daniel Oblak, as well as the Cryptography team: Philip Chan and Itzel Lucio-Martinez. I have also collaborated with individuals in University of Paderborn: Mathew George, Raimund Ricken and Prof. Wolfgang Sohler as well as in ETH Zurich: Dr. Roger Colbeck and Prof. Renato Renner. My specific contributions to each investigation will be detailed in the beginning section of each chapter.

Chapter 2

Basic Elements for Quantum Communication

In this chapter I will review the basic elements required to appreciate the following chapters. As quantum communication is based on the generation, transmission and measurement of qubits, I will review the basic mathematical properties of qubits, both single and entangled pairs, and their measurement. In each of the following sections I will also discuss some relevant experimental techniques. These techniques will be discussed in terms of photons, which are the usual candidate for quantum communication because they travel fast, generally have weak coupling to the environment, and an entire infrastructure for optical communication has already been developed.

2.1 The Qubit

Classical information is usually represented in bits: an object that can be '0' or '1'. In quantum mechanics, information is represented by the qubit: a two-level space (i.e. a system described by two orthogonal basis states) of a particle. The basis states for the qubit are usually notated as $|0\rangle$ and $|1\rangle$ (the $|\ \rangle$ is usually referred to as a *ket*, with the interior symbol identifying the specific quantum state). Departing from classical information, the quantum state of a qubit can also be a coherent superposition of its two basis states: $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, where α and β are complex numbers satisfying $\alpha^2 + \beta^2 = 1$, for normalization. Essentially, the qubit exists in both basis states simultaneously. Note that $|\psi\rangle$ will often be used to refer to an arbitrary state.

A simple graphical representation of a qubit is a vector on the Bloch sphere, see Fig. 2.1. The states $|0\rangle$ and $|1\rangle$ are represented on the poles of the sphere, and any state with $|\alpha| =$

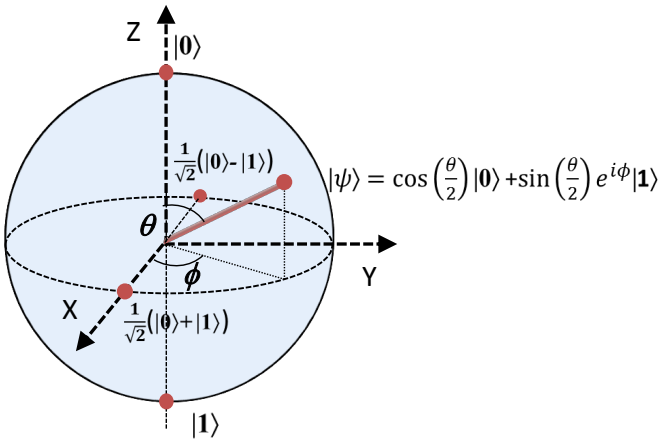


Figure 2.1: Bloch Sphere. Qubit states represented on the Bloch sphere. The parameters θ and ϕ represent the polar and azimuthal angles of the vector on the Bloch sphere that represents a qubit's quantum state.

$|\beta| = 1/\sqrt{2}$ is represented on the equator. It can be useful to write the qubit state as

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle\,, \tag{2.1}$$

where θ and ϕ can be visualized as angles from the Z- and X-axes, respectively. Note that any states represented on opposite sides of the Bloch sphere are orthogonal and hence can form a basis.

Any degree of freedom can be used to form a qubit's two-level space. With photons, polarization is a frequent choice as it is a natural two-level system with horizontal, $|H\rangle$, and vertical, $|V\rangle$, polarizations forming one possible basis (and often depicted on the poles of the Bloch sphere). Other degrees of freedom that are inherently continuous can be used to form a two-level system. A commonly used qubit is the *time-bin* qubit, in which a photon is in a superposition of two different emission times. If the time difference between these emission times is large compared to the coherence time of the photon, then orthogonal basis states are well described by time windows (temporal modes) centred on each emission time. Typically these basis states are referred to as $|early\rangle$ and $|late\rangle$, or $|t_0\rangle$ and $|t_1\rangle$. Similar principles apply to other degrees of freedom such as path or frequency.

Experimentally generating a photonic qubit begins with generating a single photon. In

principle this can be done with single emitters such as trapped atoms and ions or quantum dots. In practice these are difficult to realize and thus close approximations to single emitters are used. One technique is to attenuate a laser pulse to the single-photon level. However, as photon-number statistics from a laser follow a poissonian distribution (i.e. the probability of finding n photons in a pulse is $P(n) = \mu^n e^{-\mu}/n!$, where μ is the mean photon number), the average emission probability must be kept low to minimize multi-photon emissions. On the other hand, this creates a large number of emissions containing no photons, so called *vacuum* emissions. Another common technique is to use a non-linear process, such as spontaneous parametric down-conversion (SPDC), spontaneous four-wave mixing (SFWM) or atomic ensembles, to generate a pair of photons. By detecting one photon of this pair one can be sure of the existence of the second photon, essentially removing vacuum emissions. However, these processes are also probabilistic, following either poissonian or thermal photon-number distributions, and thus multi-photon emissions are still a concern. Nevertheless, these techniques generate approximations to single photons that suffice for many fundamental tests of quantum mechanics and applications of quantum information science.

After generating a "single" photon, it is usually straightforward to create the desired qubit state. The polarization state can be manipulated with traditional polarization optics, such as wave plates and polarizers. For time-bin qubits the qubit state can be generated with an imbalanced interferometer, such that the photon exits the interferometer in a superposition of two temporal modes in the state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|t_0\rangle + e^{i\phi}\,|t_1\rangle) \tag{2.2}$$

where ϕ is determined by the temporal distance between the two states and is typically set to zero by appropriately defining $|t_0\rangle - |t_1\rangle$. Alternatively, if the coherence time of the photon is sufficiently long, one can also *carve* two temporal modes with an intensity modulator. This also places the photon in a coherent superposition of the two temporal modes.

2.2 Measurement

In general, the state of a qubit before measurement cannot be determined. Moreover, the quantum state of a qubit is disturbed or altered through the act of measurement. These facts are captured by the most common measurement performed on photonic qubits, the *projection measurement*. Through measurement a quantum state is *projected* onto, or found in, one of the basis states of a chosen basis (and the qubit remains in that state unless there is significant evolution). For example, if the experimenter uses the basis spanned by $\{|\psi_0\rangle, |\psi_1\rangle\}$ to measure a qubit in state $|\psi\rangle$, he will project the qubit onto $|\psi_i\rangle$ with probability

$$P(|\psi_i\rangle) = |\langle\psi_i|\,|\psi\rangle|^2. \tag{2.3}$$

If the initial state $|\psi\rangle$ is a basis state of the measurement, then the outcome is deterministic and the initial state is projected onto itself with 100% certainty. For example, if the state $|0\rangle$ is measured in the $\{|0\rangle, |1\rangle\}$ basis, it is projected onto $|0\rangle$ with 100% certainty. This is essentially equivalent to the measurement of classical bits. On the other hand, if the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (known as the *plus* state) is measured in the $\{|0\rangle, |1\rangle\}$ basis, it is projected onto each basis state with probability $|\frac{1}{\sqrt{2}}|^2 = 0.5$. The same is true for the state $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. On the other hand, again departing from classical information, if the state $|+\rangle$ is measured in the $\{|+\rangle, |-\rangle\}$ basis, it will project onto $|+\rangle$ with 100% probability.

Experimentally, projection measurements with polarization qubits are straightforward to perform. A polarizing beamsplitter (PBS), which transmits horizontally polarized light and reflects vertically polarized light, followed by single-photon detectors (SPD) performs a projection measurement in the $\{|H\rangle, |V\rangle\}$ basis. Preceding these apparata with wave plates allows projections in any basis. Projecting time-bin qubits in the $\{|t_0\rangle, |t_1\rangle\}$ basis is straightforwardly done with an SPD and a module to record the time of detection. Measurements in superposition bases require an interferometer to interfere $|t_0\rangle$ and $|t_1\rangle$ before detection.

2.3 Density Matrices

So far, in this chapter, we have discussed *pure* quantum states. Pure quantum states are states that can be fully described by a single ket vector. Often in experiments this is not sufficient and the quantum state of a particle must be described by a statistical mixture of pure quantum states. These are known as *mixed states*. A mixed state cannot be represented as a ket, but is instead represented as a density matrix (note that pure states can also be represented as density matrices). The density matrix is defined as,

$$\rho = \sum_n p_n \left|\psi_n\right\rangle \left\langle\psi_n\right|, \tag{2.4}$$

where p_n is the probability that the particle is in the pure state $|\psi_n\rangle$, and n sums over all basis states in some basis. As an example, the density matrix for an even statistical mixture of the pure quantum states $|0\rangle$ and $|1\rangle$ (i.e. 50% of each) is easily calculable:

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{2.5}$$

On the other hand, the density matrix for a coherent superposition of $|0\rangle$ and $|1\rangle$, say the pure state $|+\rangle$, when written in the $\{|0\rangle, |1\rangle\}$ basis, is

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \tag{2.6}$$

The difference between these density matrices clearly indicates the fundamental difference between a statistical mixture and a quantum superposition. In general, the diagonal elements of a density matrix equal the probability to project the qubit onto the corresponding basis state while the off-diagonal elements are related to the quantum coherence between the basis states.

Addressing projective measurements more generally, the probability to project a particle in state ρ onto the pure state $|\psi\rangle$ is

$$P(|\psi_i\rangle) = \mathrm{Tr}(|\psi_i\rangle \langle\psi_i| \rho). \tag{2.7}$$

2.4 Multiple Qubits and Entanglement

Multiple independent qubits, labelled A and B, are generally represented as

$$|\psi\rangle_{AB} = |\psi_A\rangle \otimes |\psi_B\rangle \,. \tag{2.8}$$

Or more simply stated

$$|\psi\rangle_{AB} = |\psi_A\rangle \, |\psi_B\rangle \,. \tag{2.9}$$

Or even simpler

$$|\psi\rangle_{AB} = |\psi_A \psi_B\rangle \,. \tag{2.10}$$

In this case, the state of qubit A is clearly separate from the state of qubit B. It is clear that the two qubits are in independent states. These are known as *product states* or *separable states*.

On the other hand, entanglement arises when two particles cannot be written as a product state of their two individual systems (for pure states):

$$|\psi_{AB}\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle \,. \tag{2.11}$$

The four most-commonly referred to maximally entangled qubits states are known as the Bell states:

$$\left|\phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \tag{2.12}$$

and

$$\left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{2.13}$$

and these form a basis for the space of all two-qubit states. One can see that entanglement is essentially multi-qubit quantum superposition. For example, the entangled state $|\phi^+\rangle$ is a coherent superposition of both particles being in the $|0\rangle$ state and both particles being in the $|1\rangle$ state.

Moreover, by examining each qubit individually, the presence of individual randomness becomes obvious. To do this, we must first introduce the *partial trace*, which is the mathematical operation of removing, or losing, one qubit from the description. In general, there is no way to remove one particle and retain a pure state, and so we must use density matrices. The partial trace of ρ_{AB} over system B is defined as

$$\begin{aligned} \rho_A &= Tr_B(\rho_{AB}) \\ &= \sum_i \langle i|_B \, \rho_{AB} \, |i\rangle_B \end{aligned} \tag{2.14}$$

where i sums over all basis states, $|i\rangle_B$, of any particular basis. As an example, consider the density matrix for the entangled state $|\phi^+\rangle$:

$$\rho_{AB} = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \tag{2.15}$$

By applying eq. 2.14 and tracing over system B, one ends up with the density matrix

$$\rho = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{2.16}$$

which is just an even statistical mixture of $|0\rangle$ and $|1\rangle$. Thus measurements on a single qubit of a maximally entangled pair must demonstrate perfect randomness.

Lastly, the concept of a correlation coefficient was mentioned in the previous chapter. Here we will now make this concrete. The correlation coefficient $E(m, n)$ is a measure of statistical correlation between qubit A when measured in basis m and qubit B when measured in basis n. For a projection measurement in each basis there are two possible results, corresponding to the two basis states, $\{|+1\rangle, |-1\rangle\}$, although $|+1\rangle$ and $|-1\rangle$ can be replaced with $|0\rangle$ and $|1\rangle$, $|H\rangle$ and $|V\rangle$, $|t_0\rangle$ and $|t_1\rangle$, etc. The choice of physical state does

not matter. Thus the correlation coefficient can be calculated as:

$$\begin{aligned} E(m,n) &= \sum_i a_i^m b_i^n / N \\ &= P(+1,+1) - P(+1,-1) - P(-1,+1) + P(-1,-1), \end{aligned} \tag{2.17}$$

where $P(\psi_A, \psi_B)$ is the probability to project qubit A onto state $|\psi_A\rangle$ and qubit B onto state $|\psi_B\rangle$. Correlation coefficients will be used extensively in Chapter 3.

Experiments generating entangled photons first require a source of photon pairs. Photon pair sources used in the first entanglement experiments [13, 14] were made from atomic cascades (two-photon transitions in various atoms) whereas now the most commonly used source of photon pairs is SPDC in nonlinear crystals (mentioned above). To generate entanglement one needs to use the source in such a way that there exists two "paths" for pair creation to occur, which can then be superimposed. For example, in Type-I SPDC downconversion can occur only if an optical pump beam is polarized along a certain axis of the crystal. Then, if SPDC occurs, each photon of a generated pair is polarized orthogonally to the pump light. In an early SPDC entanglement source [61] two identical Type-I SPDC crystals were placed back-to-back, but with the optical axis of the second crystal at 90° with respect to the first (see Fig. 2.2). For the sake of explanation, assume that the crystals' axes are oriented horizontally and vertically, respectively. Then, pump light polarized at 45° with respect to each of the optical axes (say plus polarized) is equally likely to downconvert in either crystal. If downconversion occurs, and the crystals are thin enough so that it is impossible to determine in which crystal downconversion occurred, the downconverted light is in a superposition of being created in the first crystal and the second crystal. Thus, one has the polarization entangled state $\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$. A more common technique today is to use a Sagnac interferometer in conjunction with SPDC crystals, as detailed in Chapter 3.

Time-bin entanglement, first demonstrated in [63], can be generated by placing an SPDC crystal after an interferometer with a large path-length difference, as in Fig. 2.3. When

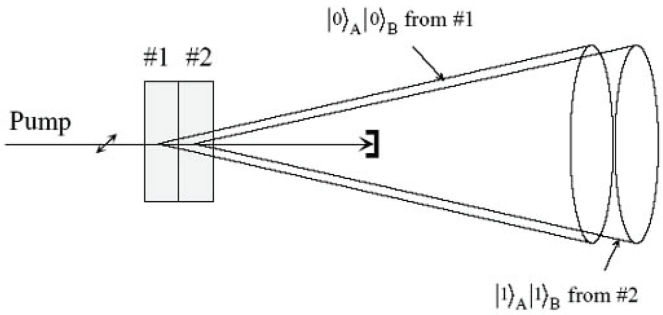


Figure 2.2: Polarization entanglement. The two crystals produce photon pairs in orthogonal polarization directions. If they are placed back-to-back then a pump polarized such that SPDC can occur in either crystal will produce entanglement. Image from [62]

suitably pulsed pump light passes through this unbalanced Mach-Zehnder interferometer it exits in a superposition of two different times (an early pulse and a late pulse). If a photon pair is produced in the source it is in a superposition of having been created by the early pulse and the late pulse, which produces the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|t_0, t_0\rangle + e^{i\phi}|t_1, t_1\rangle). \tag{2.18}$$

This time-bin entangled state is used throughout Chapter 5.

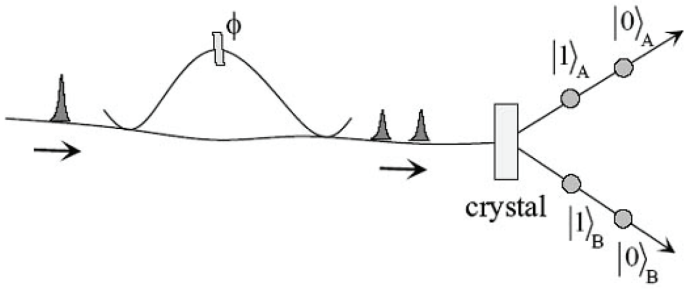


Figure 2.3: Time-Bin Entanglement. Two pulses exit the interferometer and as each are equally likely to cause down-conversion in the crystal time-bin entanglement is created. Image from [62]

2.5 Entangling Measurements

The essence of an entangling measurement is to project the state of two qubits onto an entangled state. As the four Bell states in equations 2.12 and 2.13 form a basis for all 2-qubit states, which is a 4-dimensional space, often one chooses to use this basis for entangling measurements. Hence this measurement is typically referred to as a Bell-state measurement (BSM), and will be referred to as such in following chapters.

Entanglement swapping is a simple extension of BSMs. As explained earlier, imagine two pairs of photons each in an entangled state: A entangled with B, and C entangled with D. By projecting B and C onto an entangled state, the entanglement is swapped to A and D. The final entangled state of A and D depends on the initial states of the particles as well as onto which Bell state B and C is projected. For example, if both pairs are initially in states $|\phi^+\rangle$, and B and C are then projected onto $|\psi^-\rangle$, then A and D are found in the state $|\psi^-\rangle$ as well. However, as B and C were not entangled initially they are equally likely to be projected onto any of the four Bell states. Hence, before the entanglement between A and D can be used there needs to be classical communication informing A's and D's locations of the result of the BSM and thus which entangled state they share. This is important as without the necessity of classical information, entanglement swapping would allow for faster-than-light communication.

As entanglement can be seen as two-particle superpositions, entangling measurements can similarly be seen as two-particle interference measurements. As such interference can only be observed between indistinguishable particles, it is experimentally useful to have a simple test of the indistinguishability of photons. The simplest two-particle interference measurement (see Chapters 4 and 5), known as Hong-Ou-Mandel (HOM) interference [64], involves interfering two photons on a beamsplitter. If the photons enter via different input ports and are indistinguishable, they bunch and leave together by the same output port. This is due to destructive interference between "paths" associated with both photons be-

ing transmitted and both being reflected. As no such interference occurs for photons that are distinguishable (in polarization, time or frequency), the presence of HOM interference with high visibility confirms the suitability of two photons for more advanced two-photon interference measurements, such as BSMs.

Similar to HOM interference, BSMs can also be performed by overlapping two photons on a beamsplitter (BS), and then projecting each qubit onto orthogonal states (e.g. one photon onto $|0\rangle$ and one photon onto $|1\rangle$). The act of overlapping the photons on the beamsplitter erases the *which-way* information and makes it impossible to determine which photon came from which input. By projecting each photon onto an orthogonal state one has projected their joint state onto a superposition between $|01\rangle$ and $|10\rangle$, with the phase between the two components determined by the number of reflections on the beamsplitter. If both photons are found on the same side of the BS the projected state is $|\psi^+\rangle$ and if both photons are found on opposite sides, the projected state is $|\psi^-\rangle$. The single-qubit projection measurements on each output of the beamsplitter are usually $|H\rangle$ and $|V\rangle$ for polarization qubits and $|t_0\rangle$ and $|t_1\rangle$ for time-bin qubits. In this experimental scheme, the remaining two measurement results are the unentangled $|00\rangle$ and $|11\rangle$ states, corresponding to detecting the two photons in the same state. In general, the probability for a BSM to result in a projection onto an entangled state is at most 50% when limited to linear optics [65].

Chapter 3

Quantum Entanglement for Fundamental Tests

Quantum entanglement has been, and will continue to be, at the heart of most fundamental tests of quantum mechanics. The local randomness and yet perfect correlation demonstrated by distant two-qubit entanglement has been used to convincingly rule out the existence of local realistic theories. After forty years since the first Bell inequality test, and with many believing that the first loophole-free Bell will be achieved soon, physicists are beginning to turn to more exotic fundamental tests [27, 28, 29, 66].

The standard approach has been to develop the elements of an alternative theory and then search for an experiment where the alternative theory and quantum mechanics predict different results. Bell's local hidden variables with Bell's inequalities and, more recently, Leggett's non-local hidden spin vector [27] (more detail in this chapter) with corresponding inequalities [28, 29] are both examples. For some alternative theories, such as Bohm's pilot-wave theory [67], no such differences may be possible.

An important motivation for the projects described in this chapter was to approach the problem from a general perspective. Rather than designing an alternative theory and an appropriate inequality, would it be possible to experimentally test the validity of any possible alternative theory? Can we bound the properties of alternative theories in a useful way? Following the theoretical work in [68] the answer turned out to be yes. Quantum mechanics says that the outcomes of measurements on members of entangled qubits are completely random and unpredictable before measurement – said differently, the predictive power of quantum mechanics on these measurements is zero. On the other hand, Einstein's vision and Bell's local hidden variables were deterministic and thus had maximal predictive power. The work in [68] theoretically shows how one can bound the predictive power of any

theory for entangled particles. If that bound happens to be zero, then quantum mechanics is maximally predictive and no alternative theory could do better. As with any experiments on the foundations of quantum mechanics, the results are based on the strength of a series of correlations measurements on entangled pairs and quantified through correlation coefficients.

To be more specific about our test of predictive power of alternative theories, we must first describe the experimental scenario under consideration. Imagine a source of two entangled qubits that sends each qubit to a different measurement device. These measurement devices can take as input measurement settings, A and B (which can be thought of as bases for projection measurements), and output measurement outcomes, X and Y (where $X, Y \in [\pm 1]$). Knowing the state of the two particles and the measurement apparatus one can use quantum mechanics to calculate the probability distribution of the measurement outcome X. For example, if the two particles were in a maximally-entangled state, then quantum mechanics says that the measurement outcome probability distribution P_X is uniform, regardless of the input measurement settings A and B, which means that the measurement outcomes X are completely random and unpredictable, i.e. $P_X = P_{X|AB} = P_{\bar{X}}$, where $P_{\bar{X}}$ is the uniform distribution. Now, let us suppose that there exists another, potentially hidden, property of the qubit Ξ that we could in principle measure (with input C) and determine its value, Z. Our goal then is to develop a test for the existence of any property that allows one to predict the measurement outcomes X better than quantum mechanics (see Sec. 4.2).

As mentioned above, the first example of work towards answering this question was the work of Bell [3]. However, Bell assumed that this hidden property was solely influenced by local effects and that the property would completely determine the measurement outcome X (e.g. there exists an x_0 such that $P_{X=x_0|Z} = 1$). Both of these conditions impose strict restraints on the types of hidden properties under test by Bell inequalities (commonly known as local hidden variables).

For the development of our test, our goal was to use as few assumptions as possible

about the hidden property – allowing our work to be as generally applicable as possible. The one assumption we make is that our choice of measurement setting A must be free. Specifically, that A is uncorrelated with all other values in the experiment (obviously, save X), i.e. $P_{A|BCYZ} = P_A$. As we show in the Appendix A.1, if the measurements on the two particles are space-like separated, this statement is equivalent to requiring no-signalling within the experiment. Therefore, the test we develop does not apply to any signalling hidden property, such as Bohmian hidden pilot waves [67], but does apply to any non-local or local property..

Our test, presented in section 3.2, allows one to bound the predictive power of alternative physical theories. Specifically, the predictive power δ of an alternative theory with hidden property Ξ can be defined as the statistical distance between $P_{Z|abcx}$ and $P_{Z|abc}$. (note that the lower case denotes a particular instance of the associated upper case variable) On the intuitive level, if these distributions are equal, Z and X must be uncorrelated and thus Z has no predictive power about on X. This statistical distance we use is the standard statistical $\mathcal{L}_1$ norm [69], known as the variational distance, $D(P_W, Q_W) := \frac{1}{2}\sum_x |P_W(w) - Q_W(w)|$, which has the operational interpretation: if two distributions have variational distance δ, then the average difference between the probabilities that the two probability distributions P_W and Q_W can assign to the same event is δ – said differently, the probability that we notice a difference between them is at most δ.

This chapter contains two articles. In the first article we describe the development of a new source of polarization entangled photon pairs based on two crystals in a Sagnac interferometer. The photon pairs are non-degenerate in wavelength, with one photon's wavelength at 800 nm for ease of detection and one photon's wavelength at 1550 nm for long-distance fibre transmission. The high-quality entanglement from the source is verified through quantum state tomography, which we use to we reconstruct the two-qubit density matrix, and then violations of a series of increasingly stringent inequalities (Bell inequalities and finally

a Leggett inequality).

In the second article we use the same source to bound the predictive power of any alternative theory to quantum mechanics. This test is the first of its kind as it rules out general non-local hidden variable models. Our test exhibits the standard free-choice and detection loopholes but our hope is that work with these general tests will continue and lead to higher fidelity entanglement sources and closing loopholes.

In this chapter, the experimental work was conducted in collaboration with members of the QC2 Entanglement team: Terence Stuart and Félix Bussières. I contributed to these studies in the following stages: developing the source of entanglement, as well as performing the measurements and analyzing the results. The theory was developed by Dr. Roger Colbeck and Prof. Renato Renner.

A Flexible Source of Non-Degenerate Entangled Photons Based on a Two-Crystal Sagnac Interferometer

Terence E. Stuart,[1] Joshua A. Slater,[1] Félix Bussières,[1,2] and Wolfgang Tittel[1]

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

[2] *GAP-Optique, Université de Genève, Geneva, Switzerland, CH-1211 Genève 4*

(Dated: August 25, 2013)

Sources of entangled photon pairs are a key component in both fundamental tests of quantum theory and practical applications such as quantum key distribution and quantum computing. In this work, we describe and characterize a source of polarization entangled photon pairs based on two spontaneous parametric down-conversion (SPDC) crystals in a Sagnac interferometer. Our source is compact and produces high-quality entangled states in a very flexible manner. The wavelengths of the photon pairs, around 810 and 1550 nm, the phase between orthogonal components of the entangled state, and the tangle of the state are all independently adjustable. In addition to presenting basic characterization data, we present experimental violations of CHSH and Leggett inequalities, as well as an instance of the "beautiful" Bell inequality, which has not previously been tested experimentally.

INTRODUCTION

Over the last century quantum theory has fundamentally changed our understanding of the universe and continues to offer new insights into nature. Schrödinger described entanglement as "*the* characteristic trait of quantum mechanics"[1]. As such, it is not surprising that sources of entangled particles are a key resource in experiments that probe aspects of quantum theory [2]. They are also fundamental building blocks for practical applications of quantum information theory, such as quantum key distribution [3] and linear optical quantum computing [4]. Sources of entangled photon pairs based on SPDC in non-linear crystals [5] are now widely used, and several high performance entanglement sources have been based on a non-linear crystal in a Sagnac interferometer thanks to this type of interferometer's intrinsic phase stability [6]. However, due to problems arising from chromatic dispersion in polarization optics, such sources are challenging to build if the members of the entangled pairs are generated at widely different wavelengths. One way to overcome this problem is to use periscopes instead [7]. Here we resort to another approach, which is based on a Sagnac interferometer that includes two SPDC crystals. In addition to being compact and highly flexible in terms of the states it can produce, an interesting added feature is that the quality of entanglement (the tangle) can be varied in a controlled manner. Our source has proved suitable for fundamental tests of quantum theory, some of which have not been performed before, and would also be well suited to applications requiring transmission of entangled photons through both optical fiber and free space, e.g. for hybrid quantum networks.

SOURCE DESIGN

Figure 3.1.1 shows the design of our entanglement source. Depending on the experiment, light from a 532 nm pulsed or continuous wave laser is linearly polarized before being rotated to an equal superposition of horizontal and vertical polarizations using a $\frac{\lambda}{2}$ waveplate. Pump light is then split into two paths by a polarizing beam splitter (PBS). In the clockwise (CW) branch of the interferometer, horizontally polarized pump light first encounters a periodically poled lithium niobate (PPLN) crystal that is oriented to satisfy the phase matching conditions for SPDC with vertically polarized pump light. The pump light will thus pass through this crystal without interaction because the phase matching conditions are not met at this polarization. The second PPLN crystal encountered by pump light in this path is oriented to down-convert horizontally polarized pump light, so pairs of horizontally polarized photons at non-degenerate wavelengths of 810 nm and 1550 nm are now produced. These pairs are transmitted through the PBS and exit the source. The counter-clockwise (CCW) path is similar, except that vertically polarized pairs are produced in the second crystal encountered and then reflected into the same output mode as the horizontal pairs from the CW path. The pump intensity is adjusted so that single photon-pair events dominate detection statistics, as evidenced by the results shown below. Since pump light travels through both arms of the interferometer in a coherent superposition, recombining both arms on the PBS produces the entangled state,

$$|\Phi^{\phi}\rangle = \frac{1}{\sqrt{2}}\left(|HH\rangle + e^{i\phi}|VV\rangle\right). \tag{1}$$

The phase, ϕ, is controlled using a Babinet-Soleil phase

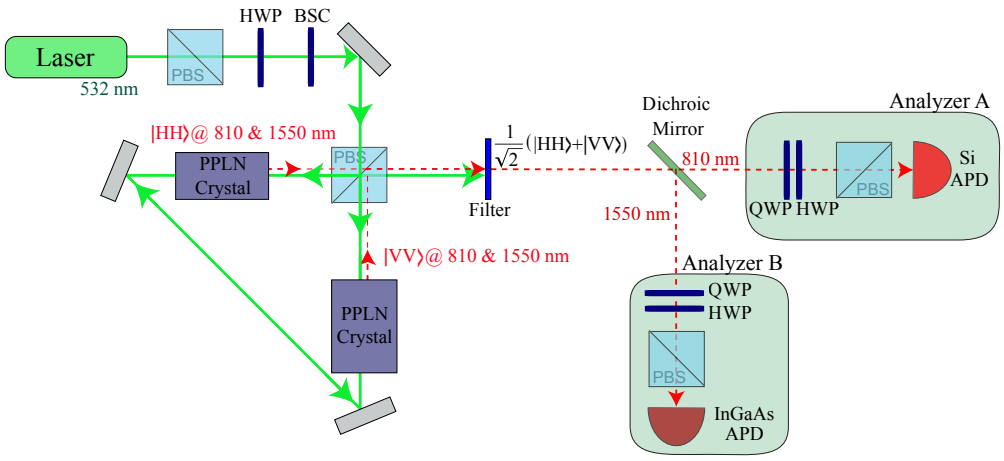


FIG. 3.1.1. **Polarization entanglement source with qubit analyzers.** Entangled states produced by the source are split according to wavelength on a dichroic mirror and distributed to analyzers A and B, which are each composed of a $\frac{\lambda}{4}$ waveplate (QWP), a $\frac{\lambda}{2}$ waveplate (HWP), polarizing beam splitter (PBS) and wavelength specific single photon detectors (Si APD and InGaAs APD). See text for details.

compensator (BSC) placed in front of the interferometer, which allows changing the phase between the horizontally and vertically polarized components of the pump laser. For the data collected for this article, ϕ was chosen to be close to zero so that the resulting state had a high fidelity with a $|\Phi^+\rangle$ Bell state.

After the pump light is filtered out, photon pairs are separated according to wavelength by a dichroic mirror and sent to wavelength specific qubit analyzers consisting of a $\frac{\lambda}{4}$ waveplate, a $\frac{\lambda}{2}$ waveplate, a PBS, and wavelength specific detectors, as shown in Figure 3.1.1. These analyzers allow arbitrary projection measurements to be made on each of the photons. A free running silicon avalanche photo-diode (Si APD) is used in the 810 nm photon analyzer, A. Its output is used to trigger an Indium Galium Arsenide (InGaAs) APD used in the 1550 nm analyzer, B. Detection signals are collected using a Time-to-Digital Converter (TDC) so that coincidences between detection events can be recorded. Using approximately 2 mW of pump power, signal photon detections occur at a rate of approximately 20 KHz and coincidences at a rate of approximately 500 Hz. The dark count rate for the Si APD is approximately 40 Hz, and the InGaAs APD has a dark count rate of $5\text{x}10^{-5}$/ns.

VISIBILITY AND QUANTUM STATE TOMOGRAPHY

Two-photon interference visibilities were assessed by performing two sets of measurements using the continuous wave pump laser. In the first measurement analyzer A (810 nm) projected onto $|H\rangle$ while the analyzer B (1550 nm) projected onto states represented on the great circle around the Bloch sphere that includes $|H\rangle$, $|V\rangle$, $|+\rangle$, and $|-\rangle$. In the second measurement, the analyzer A projects onto $|+\rangle$ and the analyzer B projects onto states represented on the great circle including $|R\rangle$, $|L\rangle$, $|+\rangle$, and $|-\rangle$. Here, $|+\rangle$ and $|-\rangle$ denote $\pm$ 45^o linear polarization, and $|R\rangle$ and $|L\rangle$ denote right and left circular polarization, respectively. Fitting the measured coincidence rates to sinusoidal functions with visibilities V_1 and V_2, we find $V_1 = (99.1\pm0.7)\%$ and $V_2 = (97.4\pm0.9)\%$, both being close to the maximum value of 100%.

Table 3.1.1 shows data of a typical density matrix resulting from maximum likelihood quantum state tomography (QST) [8] with a tangle [9] of $\mathcal{T} = 0.905$.

(a) $Re\{\rho\}$

	$\langle HH\|$	$\langle HV\|$	$\langle VH\|$	$\langle VV\|$
$\|HH\rangle$	0.5085	0.0085	-0.0151	0.4773
$\|HV\rangle$	0.0085	0.0028	-0.0006	0.0145
$\|VH\rangle$	-0.0151	-0.0006	0.0038	-0.0075
$\|VV\rangle$	0.4773	0.0145	-0.0075	0.4848

(b) $Im\{\rho\}$

	$\langle HH\|$	$\langle HV\|$	$\langle VH\|$	$\langle VV\|$
$\|HH\rangle$	0.0000	0.0028	-0.0027	-0.0337
$\|HV\rangle$	-0.0028	0.0000	0.0028	0.0036
$\|VH\rangle$	0.0027	-0.0028	0.0000	-0.0045
$\|VV\rangle$	0.0337	-0.0036	0.0045	0.0000

TABLE 3.1.1. **Typical Density Matrix.** Real and imaginary parts of the density matrix generated by maximum likelihood QST performed when the spectral overlap between SPDC crystals was optimized. The tangle is($\mathcal{T} = 0.905$).

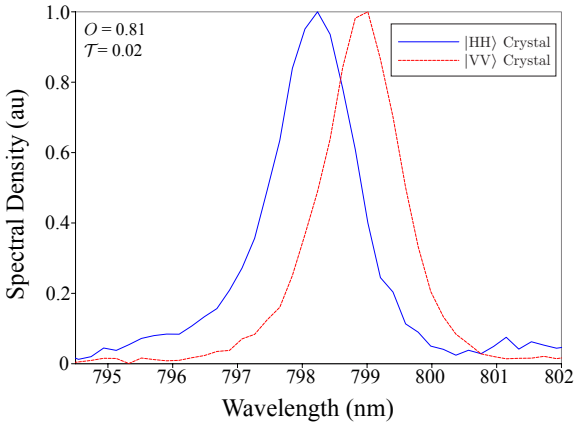


FIG. 3.1.2. **Single photon spectra for two crystals at different temperatures.** This plot shows single photon spectra gathered for $\sim 810\ nm$ signal photons from the entanglement source's $|VV\rangle$ PPLN crystal at $T = 165.70\ ^{\circ}C$ and from the $|HH\rangle$ PPLN crystal at $T = 165.20\ ^{\circ}C$.

CONTROLLING TANGLE

In order for the entangled state produced by this source to be of high quality (i.e. to have a tangle close to 1), the spectra produced by the two SPDC crystals must match as closely as possible. Imperfectly overlapping spectra yield information that reveals in which crystal a given pair of photons was created, thus reducing the tangle of the state. The crystals used were made by the same manufacturer, but at different times and therefore have slightly different poling periods if they are at the same temperature. By maintaining the SPDC crystals at slightly different temperatures we can select the phase-matching conditions such that the spectra of the $|HH\rangle$ and $|VV\rangle$ photon pairs are nearly indistinguishable. This changes the phase ϕ of the state in eq. 1, which we compensate for using the BSC. It is also possible to deliberately mismatch the spectra in a controlled way, allowing this source to produce states with an arbitrary degree of entanglement. This is done by adjusting the temperature of one PPLN crystal relative to the other, thus altering the spectrum of photons it produces and reducing the spectral overlap between pairs produced by the two SPDC crystals.

Figure 3.1.2 shows two signal spectra one gathered from the $|HH\rangle$ PPLN crystal at $T = 165.2\ ^{\circ}C$ and the other gathered from the $|VV\rangle$ PPLN crystal at $T = 165.70\ ^{\circ}C$. For these temperatures the two spectra have incomplete overlap O (see equation 2), and the tangle $\mathcal{T}$ of the photon pairs produced is small, but non-zero. Note that the data presented in this section has been taken with the pulsed pump; all other data has been taken with the continuous wave laser.

To see how tangle is related to spectral overlap, we then

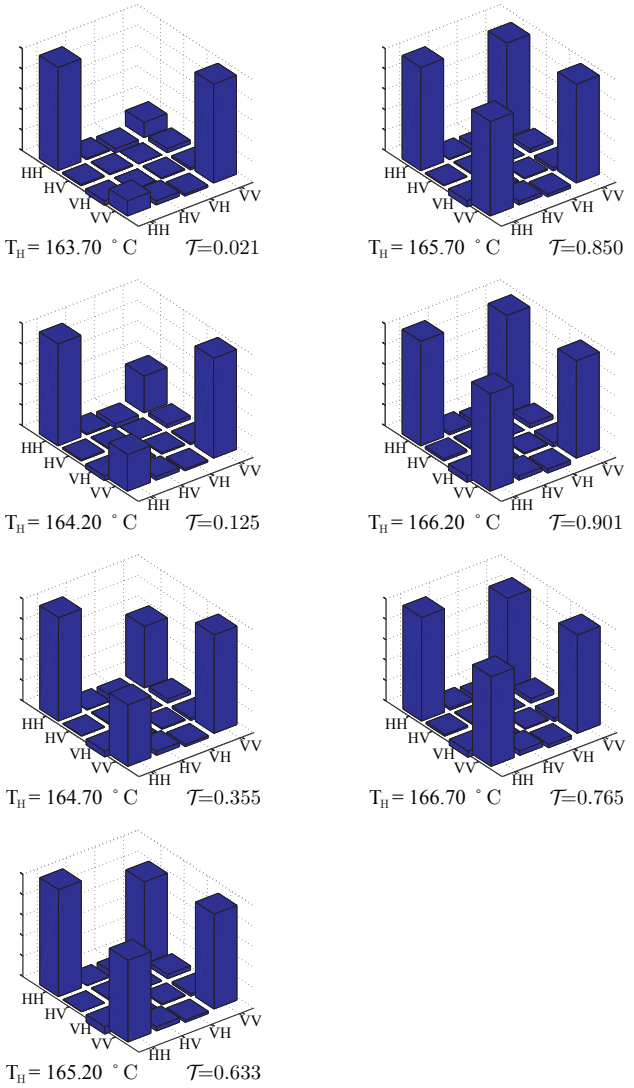


FIG. 3.1.3. **Density matrices for different temperatures.** This plot depicts the real components of the density matrices shown from each data point in Figure 3.1.4, ordered column wise by crystal temperature. Full density matrices for each point are detailed in Table 3.1.2.

varied the temperature of the PPLN crystal that down-converts pump light in the CW path of our entanglement source while the other SPDC crystal's temperature was held constant. This shifted the spectrum of the $|HH\rangle$ component of the state relative to the $|VV\rangle$ component, resulting in different degrees of spectral overlap, O, which we calculate as:

$$O = \int \sqrt{S_{HH}(\lambda)}\sqrt{S_{VV}(\lambda)}d\lambda. \qquad (2)$$

where $S_{HH}(\lambda)$ is the the signal spectral density as a function of wavelength, λ, for the SPDC crystal producing $|HH\rangle$ photons pairs and $S_{VV}(\lambda)$ is the signal spectral density of the SPDC crystal producing $|VV\rangle$ photon

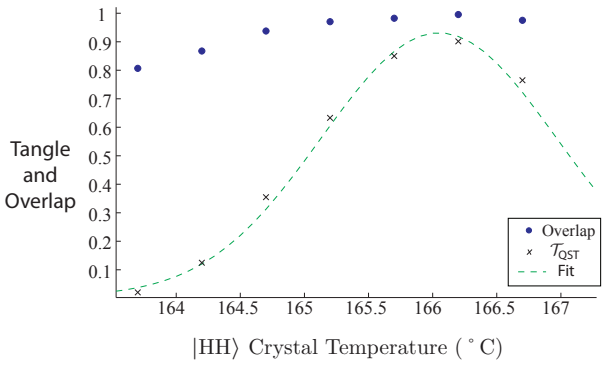


FIG. 3.1.4. **Tangle vs spectral overlap.** This plot shows tangles derived from density matrices (shown in Table 3.1.2) measured via QST, $\mathcal{T}_{QST}$, as the spectral overlap was changed by varying the temperature of the $|HH\rangle$ PPLN crystal. The $|VV\rangle$ crystal's temperature was kept constant. Also shown is the overlap, O, of the measured spectra.

pairs.

We measured the spectrum of the signal photons from the $|VV\rangle$ SPDC crystal, which was kept at a constant temperature of $T = 165.70\ ^\circ C$ using a temperature controlled oven that is stable to $\pm\ 0.01\ ^\circ C$. We also measured spectra of signal photons from the $|HH\rangle$ SPDC crystal at several different temperatures. At each of these temperatures we also performed QST on the resulting bipartite states to find density matrices and associated tangles for each temperature as shown in Figure 3.1.3. Tangle and overlap vs crystal temperature are shown in Figure 3.1.4.

TESTS OF CHSH BELL, "BEAUTIFUL" BELL, AND LEGGETT INEQUALITIES

Bell inequalities

To assess the non-classical properties of the states produced by our source we first tested the CHSH Bell inequality [10]. A violation of this inequality demonstrates that local hidden variable (LHV) models are not adequate to describe the behaviour of the states the source is producing and demonstrates the presence of entanglement. In the CHSH inequality, Alice and Bob each measure in one of two bases, chosen uniformly and at random. For each combination of bases, $\hat{a}_i = \{a_i, a_i^\perp\}$ and $\hat{b}_j = \{b_j, b_j^\perp\}$, Alice and Bob measure the correlation coefficient,

$$\begin{aligned} E(\hat{a}_i, \hat{b}_j) =& P(a_i, b_j) + P(a_i^\perp, b_j^\perp) \\ & - P(a_i^\perp, b_j) - P(a_i, b_j^\perp), \end{aligned} \tag{3}$$

where:

$$P(a_i, b_j) = \frac{C(a_i, b_j)}{C(a_i, b_j) + C(a_i^\perp, b_j) + C(a_i, b_j^\perp) + C(a_i^\perp, b_j^\perp)}$$

and $C(a_i, b_j)$ is the number of "coincidence" detections observed when Alice and Bob projectively measure along basis vectors a_i and b_j respectively. One optimal set of bases for testing a the CHSH Bell inequality with a $|\Phi^+\rangle$ state is shown in Figure 3.1.5. We then calculate the Bell S parameter as:

$$\begin{aligned} S =& E(\hat{a}_1, \hat{b}_1) - E(\hat{a}_1, \hat{b}_2) \\ & + E(\hat{a}_2, \hat{b}_1) + E(\hat{a}_2, \hat{b}_2). \end{aligned} \tag{4}$$

LHV models predict that S must fall within the range: $-2 \leq S \leq 2$. Measurements made with our source (again using the continuous wave laser) produced a value of $S = 2.757 \pm 0.008$. The uncertainty is based on Poissonian statistics. We note that QST yielded a density matrix with a tangle of $\mathcal{T} = 0.884$ immediately before this measurement. Based on this we would expect a maximum S parameter value of $S_{max} = 2\sqrt{1+\mathcal{T}} = 2.75$, which is consistent with the measured value.

In the CHSH Bell inequality two particles, each with a Hilbert space of dimension $m = 2$, are distributed to Alice and Bob. Alice makes projective measurements onto 4 states in $n = 2$ bases. For an optimal violation of the bound given by the inequality, Alice chooses bases that are mutually unbiased and Bob makes projective measurements onto all $m^n = 4$ possible intermediate states (see [12] for a precise definition). An interesting question is if (and how) Bell inequalities can be constructed that

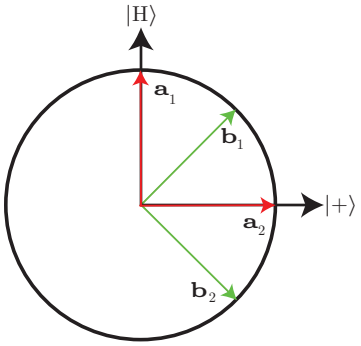


FIG. 3.1.5. **CHSH Measurement Bases.** An optimal set of measurement bases for testing the CHSH Bell inequality when using a $|\Phi^+\rangle$ state is shown here on the equator of the Bloch sphere. Only one vector for each basis is shown. The orthogonal vector associated with each basis is rotated by π from the vector shown.

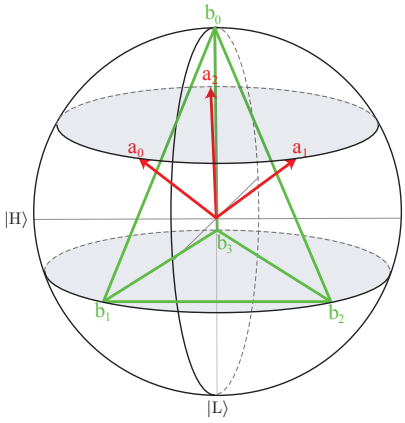


FIG. 3.1.6. **Beautiful Bell measurement bases.** Alice measures in three mutually unbiased bases $\{\hat{a}_0, \hat{a}_1, \hat{a}_2\}$ and Bob measures in bases $\{\hat{b}_0, \hat{b}_1, \hat{b}_2, \hat{b}_3\}$ [13]. Only one basis vector (e.g. a_1 from $\hat{a}_1 = \{a_1, a_1^{\perp}\}$) from each basis is shown.

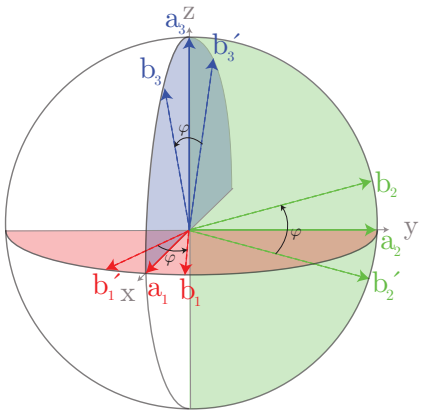


FIG. 3.1.7. **Leggett Measurment Settings.** Settings used by Alice (solid lines) and Bob (dashed lines) to test the Leggett inequality. b_1 and b_1' are each separated from a_1 by $\frac{\varphi}{2}$, and by φ from each other in the XY plane. Similarly, b_2 and b_2' lie in the YZ plane and b_3 and b_3' are in the XZ plane.

a) make use of higher-dimension states or larger number of measurements made by Alice, and b) require similarly symmetric projection measurements for maximum violation. The "beautiful" Bell family of inequalities [11] was proposed by H. Bechmann-Pasquinucci and N. Gisin in 2003 [12] and expanded upon by Gisin in 2008 [13] in response to these questions. The authors proposed a general form of Bell inequalities, parametrized by m and n, for which the CHSH Bell inequality is the specific case in which $m = 2$ and $n = 2$. The next simplest (and only) inequality in the "beautiful" Bell family that we can evaluate with a source of entangled qubits is the $m = 3$, $n = 2$ case. This inequality differs from the CHSH Bell inequality in that Alice measures in 3 bases, each spanned by two orthogonal states. Some reflection yields $m^n = 2^3 = 8$ intermediate states that Bob needs to projectively measures onto [12]. The optimal measurement bases for the $m = 3$, $n = 2$ case are shown in Figure 3.1.6 – note their highly symmetric distribution around the Bloch sphere.

The (2,3) "beautiful" Bell inequality reads:

$$\begin{aligned} S_{BB}^{2,3} =& E(\hat{a}_0, \hat{b}_0) + E(\hat{a}_0, \hat{b}_1) - E(\hat{a}_0, \hat{b}_2) - E(\hat{a}_0, \hat{b}_3) + \\ & E(\hat{a}_1, \hat{b}_0) - E(\hat{a}_1, \hat{b}_1) + E(\hat{a}_1, \hat{b}_2) - E(\hat{a}_1, \hat{b}_3) + \\ & E(\hat{a}_2, \hat{b}_0) - E(\hat{a}_2, \hat{b}_1) - E(\hat{a}_2, \hat{b}_2) + E(\hat{a}_2, \hat{b}_3). \end{aligned}$$

Here $\hat{a}_i$ and $\hat{b}_j$ are measurement bases used by analyzers A and B respectively and $E(\hat{a}_i, \hat{b}_j)$ are correlation coefficients. LHV models predict that this inequality is bounded by $S_{BB}^{2,3} \leq 6$, while quantum theory predicts a bound of $S_{BB}^{2,3} \leq 4\sqrt{3} = 6.928$. A minimal violation of the beautiful Bell inequality requires an entanglement visibility of roughly 87%.

We measured a value of $S_{BB}^{2,3} = 6.67 \pm 0.08$ (derived from measurement results shown in Table 3.1.3), equivalent to a violation of LHV models by over 8 standard deviations. We are not aware of any previously published experimental violation of the $m = 3$, $n = 2$ (or higher dimension) "beautiful" Bell inequality.

Leggett inequality

The Leggett model [14] differs from deterministic LHV models in that it permits some non-local interactions and makes probabilistic predictions about outcomes of individual measurements. The Leggett model is interesting because experiments that rule out the LHV models do not automatically rule out NLHV models such as the Leggett model. This model was first experimentally tested in 2007 [15]. We tested the 2008 version of the Leggett inequality proposed and first violated by Branciard et al. [16], who defined

$$L_3(\varphi) \equiv \frac{1}{3} \sum_{i=1}^{3} |E(\hat{a}_i, \hat{b}_i) + E(\hat{a}_i, \hat{b}_i')|. \qquad (5)$$

Here, $E(\hat{a}, \hat{b})$ is the correlation function resulting when Alice and Bob measure in pairs of bases separated by angle φ, as shown in Figure 3.1.7. The bound provided by the Leggett model for L_3 is:

$$L_3(\varphi) \leq 2 - \frac{2}{3} |\sin \frac{\varphi}{2}| \qquad (6)$$

Figure 3.1.8 shows the results we obtained for several different values of φ. Each measured point is above the solid red line, which corresponds to the bound of the

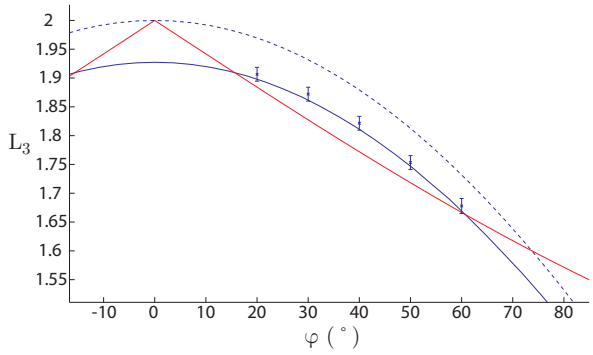


FIG. 3.1.8. **Leggett inequality measurement results.** Experimentally measured values for $L_3(\varphi)$ are shown versus φ. Points with uncertainty bars are experimentally measured values for $L_3(\varphi)$. The solid red line is the upper bound for the Leggett Model. Each experimental data point above this line is a violation of the Leggett inequality. The blue solid line shows predicted L_3 values based on a density matrix measured via QST (tangle $\mathcal{T} = 0.905$). The dashed line is the expected L_3 value for a perfect $|\Phi^+\rangle$ state.

Leggett model (equation 6) and is therefore a violation of the model. The maximal violation occurs at $\varphi = 40°$. At this setting, the measured value is $L_3 = 1.82 \pm 0.02$ while the Leggett model is bounded by 1.772 (see Table 3.1.4 in the appendix for measurements settings and results for this data point). To our knowledge, this is the first time that the Leggett inequality of the form in [16] has been violated with photon pairs at non-degenerate wavelengths. Our result confirms that the specific class of NHLV models described by Leggett is not compatible with experimental observations.

CONCLUSION

We have demonstrated a compact and highly flexible source of entangled photon pairs at widely different wavelengths that features high visibility and adjustable tangle. Our source has proved useful for several fundamental tests of quantum theory, namely violations of Bell and Leggett inequalities. It is interesting to note that these tests, which require testing specific inequalities, are not the only way to refute local or certain non-local theories that attempt to explain the origin of quantum correlations. Using the same source, we recently arrived at the same conclusion based on a more general approach [17]. More precisely, we ruled out all alternative theories to quantum mechanics, within a causal structure compatible with relativity theory, that improve on quantum mechanical predictions about the outcomes of measurements on maximally entangled particles by more than 16.5%. In particular, this rules out local and nonlocal hidden variable theories à la Bell and Leggett, respectively.

ACKNOWLEDGEMENTS

The authors thank P. Gimby, P. Irwin, and V. Kiselyov for lending material and technical support, and acknowledge funding by NSERC, Alberta Innovates Technology Futures, CFI, AAET and the Killam Trusts.

[1] Schrödinger, E. Discussion of Probability Relations between Separated Systems. *Mathematical Proceedings of the Cambridge Philosophical Society* **31:04**, 555–563 (1935).

[2] Tittle, W., Weihs, G. Photonic Entanglement for Fundamental Tests and Quantum Communication. *Quantum Information and Computation* **1:2**, 3–56 (2001).

[3] Burnham, D. C., Weinberg, D. L. Quantum cryptography based on Bell's theorem. *Physical Review Letters* **67**, 661–663 (1991).

[4] Kok, P., Munro, W. J., Nemoto, K., Ralph, T. C., Dowling, J. P., Milburn, G. J. Linear optical quantum computing with photonic qubits. *Reviews of Modern Physics* **79**, 135–174 (2007).

[5] Burnham, D. C., Weinberg, D. L. Observation of Simultaneity in Parametric Production of Optical Photon Pairs. *Physical Review Letters* **25**, 84–87 (1970).

[6] Kim, T., Fiorentino, M., Wong, F. N. C. Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer. *Physical Review A* **73**, 12316 (2006).

[7] Hentschel, M., Hübel, H., Poppe, A., Zeilinger, A. Three-color Sagnac source of polarization-entangled photon pairs. *Optics Express* **17:25**, 23153–23159 (2009).

[8] Altepeter, J. B., Jeffrey, E. R., Kwiat, P. J. Photonic State Tomography. *Advances In Atomic, Molecular, and Optical Physics* **52**, 105-159 (2005).

[9] Coffman, V., Kundu, J., Wooters, W. K. Distributed entanglement. *Physical Review A* **61**, 052306 (2000).

[10] Clauser, J. F., Horne, M. A., Shimony, A., Holt, R. A. Proposed Experiment to Test Local Hidden-Variable Theories. *Physical Review Letters* **23**, 880-884 (1969).

[11] The beautiful Bell inequality is called the "Bell inequality in arbitrary dimension" in Bechmann-Pasquinucci and Gisin's 2003 paper and the "elegant Bell" inequality in Gisin's 2008 paper.

[12] Bechmann-Pasquinucci, H., Gisin, N. Intermediate states in quantum cryptography and Bell inequalities. *Physical Review A* **67**, 062310 (2003).

[13] Gisin, N. Bell inequalities: many questions, a few answers. arXiv:0702021 (2008).

[14] Leggett, A. J. Nonlocal hidden-variable theories and quantum mechanics: An incompatibility theorem. *Foundations of Physics* **33**, 1469–1493 (2003).

[15] Gröblacher, S., Paterek, T., Kaltenbaek, R., Brukner, C., Zukowski, M., Aspelmeyer, M., Zeilinger, A. An expeirmental test of non-local realism. *Nature* **446**, 871–875 (2007).

[16] Branciard, C., Brunner, N., Gisin, N., Kurtsiefer, C., Lamas-Linares, A., Ling, A., Scarani, V. Testing quantum correlations versus single-particle properties within Leggett's model and beyond. *Nature Physics* **4**, 681–685

(2008).

[17] Stuart, T. E., Slater, J. A., Colbeck, R., Renner, R., Tittel, W. Experimental Bound on the Maximum Predictive Power of Physical Theories. *Physical Review Letters* **109**, 020402 (2012).

APPENDIX

163.70 °C

ρ_{Re}	$\langle HH\vert$	$\langle HV\vert$	$\langle VH\vert$	$\langle VV\vert$
$\vert HH\rangle$	0.5062	0.0065	-0.0211	0.0742
$\vert HV\rangle$	0.0065	0.0043	0.0001	0.0196
$\vert VH\rangle$	-0.0211	0.0001	0.0046	-0.0102
$\vert VV\rangle$	0.0742	0.0196	-0.0102	0.4849

ρ_{Im}	$\langle HH\vert$	$\langle HV\vert$	$\langle VH\vert$	$\langle VV\vert$
$\vert HH\rangle$	0.0000	-0.0110	-0.0069	0.0046
$\vert HV\rangle$	0.0110	0.0000	0.0002	0.0093
$\vert VH\rangle$	0.0069	-0.0002	0.0000	0.0115
$\vert VV\rangle$	-0.0046	-0.0093	-0.0115	0.0000

164.20 °C

ρ_{Re}	$\langle HH\vert$	$\langle HV\vert$	$\langle VH\vert$	$\langle VV\vert$
$\vert HH\rangle$	0.4995	0.0061	-0.0217	0.1798
$\vert HV\rangle$	0.0061	0.0043	0.0008	0.0164
$\vert VH\rangle$	-0.0217	0.0008	0.0059	-0.0082
$\vert VV\rangle$	0.1798	0.0164	-0.0082	0.4903

ρ_{Im}	$\langle HH\vert$	$\langle HV\vert$	$\langle VH\vert$	$\langle VV\vert$
$\vert HH\rangle$	0.0000	-0.0048	-0.0085	-0.0091
$\vert HV\rangle$	0.0048	0.0000	-0.0039	0.0125
$\vert VH\rangle$	0.0085	0.0039	0.0000	0.0092
$\vert VV\rangle$	0.0091	-0.0125	-0.0092	0.0000

164.70 °C

ρ_{Re}	$\langle HH\vert$	$\langle HV\vert$	$\langle VH\vert$	$\langle VV\vert$
$\vert HH\rangle$	0.5073	0.0027	-0.0291	0.3012
$\vert HV\rangle$	0.0027	0.0049	0.0002	0.0196
$\vert VH\rangle$	-0.0291	0.0002	0.0048	-0.0109
$\vert VV\rangle$	0.3012	0.0196	-0.0109	0.4830

ρ_{Im}	$\langle HH\vert$	$\langle HV\vert$	$\langle VH\vert$	$\langle VV\vert$
$\vert HH\rangle$	0.0000	-0.0064	-0.0043	-0.0017
$\vert HV\rangle$	0.0064	0.0000	-0.0038	0.0042
$\vert VH\rangle$	0.0043	0.0038	0.0000	0.0078
$\vert VV\rangle$	0.0017	-0.0042	-0.0078	0.0000

165.20 °C

ρ_{Re}	$\langle HH\vert$	$\langle HV\vert$	$\langle VH\vert$	$\langle VV\vert$
$\vert HH\rangle$	0.5249	0.0003	-0.0360	0.4007
$\vert HV\rangle$	0.0003	0.0045	0.0010	0.0210
$\vert VH\rangle$	-0.0360	0.0010	0.0050	-0.0111
$\vert VV\rangle$	0.4007	0.0210	-0.0111	0.4656

ρ_{Im}	$\langle HH\vert$	$\langle HV\vert$	$\langle VH\vert$	$\langle VV\vert$
$\vert HH\rangle$	0.0000	-0.0033	-0.0050	-0.0154
$\vert HV\rangle$	0.0033	0.0000	-0.0004	0.0057
$\vert VH\rangle$	0.0050	0.0004	0.0000	0.0063
$\vert VV\rangle$	0.0154	-0.0057	-0.0063	0.0000

165.70 °C

ρ_{Re}	$\langle HH\vert$	$\langle HV\vert$	$\langle VH\vert$	$\langle VV\vert$
$\vert HH\rangle$	0.5057	0.0039	-0.0301	0.4632
$\vert HV\rangle$	0.0039	0.0045	0.0025	0.0179
$\vert VH\rangle$	-0.0301	0.0025	0.0052	-0.0144
$\vert VV\rangle$	0.4632	0.0179	-0.0144	0.4846

ρ_{Im}	$\langle HH\vert$	$\langle HV\vert$	$\langle VH\vert$	$\langle VV\vert$
$\vert HH\rangle$	0.0000	-0.0028	-0.0047	-0.0264
$\vert HV\rangle$	0.0028	0.0000	-0.0005	0.0045
$\vert VH\rangle$	0.0047	0.0005	0.0000	0.0068
$\vert VV\rangle$	0.0264	-0.0045	-0.0068	0.0000

166.20 °C

ρ_{Re}	$\langle HH\vert$	$\langle HV\vert$	$\langle VH\vert$	$\langle VV\vert$
$\vert HH\rangle$	0.5125	0.0111	-0.0305	0.4770
$\vert HV\rangle$	0.0111	0.0048	0.0015	0.0197
$\vert VH\rangle$	-0.0305	0.0015	0.0051	-0.0191
$\vert VV\rangle$	0.4770	0.0197	-0.0191	0.4775

ρ_{Im}	$\langle HH\vert$	$\langle HV\vert$	$\langle VH\vert$	$\langle VV\vert$
$\vert HH\rangle$	0.0000	0.0000	-0.0029	-0.0281
$\vert HV\rangle$	0.0000	0.0000	0.0010	0.0028
$\vert VH\rangle$	0.0029	-0.0010	0.0000	0.0015
$\vert VV\rangle$	0.0281	-0.0028	-0.0015	0.0000

166.70 °C

ρ_{Re}	$\langle HH\vert$	$\langle HV\vert$	$\langle VH\vert$	$\langle VV\vert$
$\vert HH\rangle$	0.5076	0.0084	-0.0317	0.4396
$\vert HV\rangle$	0.0084	0.0052	0.0007	0.0226
$\vert VH\rangle$	-0.0317	0.0007	0.0045	-0.0157
$\vert VV\rangle$	0.4396	0.0226	-0.0157	0.4827

ρ_{Im}	$\langle HH\vert$	$\langle HV\vert$	$\langle VH\vert$	$\langle VV\vert$
$\vert HH\rangle$	0.0000	-0.0032	-0.0052	-0.0227
$\vert HV\rangle$	0.0032	0.0000	-0.0019	0.0040
$\vert VH\rangle$	0.0052	0.0019	0.0000	0.0069
$\vert VV\rangle$	0.0227	-0.0040	-0.0069	0.0000

TABLE 3.1.2. **Tangle versus Spectral Overlap Density Matrices.** Density matrices measured as $\vert HH\rangle$ SPDC crystal temperature (shown above) was varied. Phase was adjusted for maximal fidelity to a $\vert\Phi^+\rangle$ (positive values for off-diagonal terms $\vert HH\rangle\langle VV\vert$ and $\vert VV\rangle\langle HH\vert$) or $\vert\Phi^-\rangle$ (negative values for off-diagonal terms) state. The $\vert VV\rangle$ SPDC crystal temperature was kept at a constant 165.70 °C.

Bases	$E(\hat{a}_i, \hat{b}_j)$	$\Delta E(\hat{a}_i, \hat{b}_j)$	Bases	$E(\hat{a}_i, \hat{b}_j)$	$\Delta E(\hat{a}_i, \hat{b}_j)$
$\{\hat{a}_0, \hat{b}_0\}$	0.5742	0.0061	$\{\hat{a}_1, \hat{b}_2\}$	0.5763	0.0060
$\{\hat{a}_0, \hat{b}_1\}$	0.5247	0.0062	$\{\hat{a}_1, \hat{b}_3\}$	-0.5833	0.0061
$\{\hat{a}_0, \hat{b}_2\}$	-0.5641	0.0062	$\{\hat{a}_2, \hat{b}_0\}$	0.6124	0.0061
$\{\hat{a}_0, \hat{b}_3\}$	-0.5678	0.0061	$\{\hat{a}_2, \hat{b}_1\}$	-0.6255	0.0061
$\{\hat{a}_1, \hat{b}_0\}$	0.5446	0.0061	$\{\hat{a}_2, \hat{b}_2\}$	-0.5039	0.0061
$\{\hat{a}_1, \hat{b}_1\}$	-0.5307	0.0061	$\{\hat{a}_2, \hat{b}_3\}$	0.4645	0.0061

TABLE 3.1.3. **Beautiful Bell Measurement Settings and Data.** This table shows raw data collected to find $S_{BB} = 6.67 \pm 0.08 > 6$. $E(\hat{a}_i, \hat{b}_j)$ is the correlation coefficient measured using bases $\hat{a}_i$ and $\hat{b}_j$. Four coincidence measurements (not shown) consisting of 40 second samples were recorded for each correlation coefficient. Uncertainties are derived from Poissonian statistics.

Bases	$E(\hat{a}_i, \hat{b}_j)$	$\Delta E(\hat{a}_i, \hat{b}_j)$
$\{\hat{a}_1, \hat{b}_1\}$	0.9083	0.0057
$\{\hat{a}_1, \hat{b}'_1\}$	0.8919	0.0057
$\{\hat{a}_2, \hat{b}_2\}$	-0.9081	0.0038
$\{\hat{a}_2, \hat{b}'_2\}$	-0.8972	0.0059
$\{\hat{a}_3, \hat{b}_3\}$	0.9199	0.0059
$\{\hat{a}_3, \hat{b}'_3\}$	0.9391	0.0060

TABLE 3.1.4. **Leggett Inequality Data ($\varphi = 40°$).** This table shows correlation coefficients, $E(\hat{a}_i, \hat{b}_j)$, measured between bases $\hat{a}_i$ and $\hat{b}_j$ respectively to find $L_3 = 1.82 \pm 0.02 > 1.772$ for $\varphi = 40°$. Data collection time for each point was 40 seconds. Uncertainties are derived from Poissonian statistics.

An experimental bound on the maximum predictive power of physical theories

Terence E. Stuart,[1] Joshua A. Slater,[1] Roger Colbeck,[2,3] Renato Renner,[2] and Wolfgang Tittel[1]

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

[2] *Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland.*

[3] *Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada.*

The question of whether the probabilistic nature of quantum mechanical predictions can be alleviated by supplementing the wave function with additional information has received a lot of attention during the past century. A few specific models have been suggested, and subsequently falsified. Here we give a more general answer to this question: We provide experimental data that, as well as falsifying these models, cannot be explained within any alternative theory that could predict the outcomes of measurements on maximally entangled particles with significantly higher probability than quantum theory. Our conclusion is based on the assumptions that all measurement settings have been chosen freely, and that the presence of the detection loophole did not affect the measurement outcomes.

Many of the predictions we make in everyday life are probabilistic. Usually this is caused by having incomplete information, as is the case when making weather forecasts. On the other hand, even with all the information available within quantum mechanics, the outcomes of certain experiments, e.g., the path taken by a member of a maximally entangled pair of spin-half particles that passes through a Stern-Gerlach apparatus, are generally not predictable before the start of the experiment (see Fig. 3.2.1). This lack of predictive power has prompted a long debate, going back to the paper by Einstein, Podolsky and Rosen [1], of whether quantum mechanics is the optimal way to predict measurement outcomes. In turn, these discussions have led to important fundamental insights. In particular, Kochen and Specker, and independently Bell, proved that there cannot exist any *noncontextual* theory that predicts observations with certainty [2, 3]. In a similar vein, Bell showed [4] that in general there cannot exist any additional local property (a *local hidden variable*) that completely determines the outcome of any measurement on the particle. Bell's argument relies on the fact that entangled particles give rise to correlations that cannot be reproduced in a local hidden variable theory. The existence of such correlations has been confirmed in a series of increasingly sophisticated experiments [5–10], and local hidden variable models have thus been ruled out.

The purpose of the above arguments was to refute theories in which access to hidden parameters would, in principle, allow perfect predictions of the outcomes of any experiment. However, these arguments do not rule out possible theories that have more predictive power than quantum mechanics, while remaining probabilistic [11]. Consider again the Stern-Gerlach apparatus in Fig. 3.2.1 in which, according to quantum mechanics, a member of a maximally entangled particle pair may be deviated in one of two directions, each with probability 0.5. One may now conceive of a theory that, depending on a *hidden vector*, $\mathbf{z}$ which may be seen as a "classical spin"), would allow us to predict the direction of deviation with a larger probability, say 0.75, thereby improving the quantum mechanical prediction by 0.25. This corresponds to a proposal put forward by Leggett [13]. (We note that the given value of 0.75 assumes the most natural Leggett-type model, in which the direction of the hidden spin vector $\mathbf{z}$ is uniformly distributed [14]. Furthermore, we emphasize that the essence of Leggett's model is the existence of the hidden spin vector, and not whether the spin vectors of two particles are connected in a local or a non-local fashion.) As in the case of local hidden variable models, Leggett-type hidden spin models have been shown to be incompatible with quantum theory [13] and falsified experimentally [15–19].

In this letter we present experimental data that bounds the probability, δ, by which *any alternative theory* could improve upon predictions made by quantum theory about measurements on members of maximally entangled particles while being consistent with the assumption that measurement settings can be chosen freely. We find that quantum theory is close to optimal in terms of its predictive power. Our work develops a recent theoretical argument [20] that refutes alternative theories with increased predictive power based on the assumption that quantum theory is correct (similar to Bell's and Leggett's arguments [4, 13]), and is itself based on a sequence of work [21–24]. Here we experimentally investigate this assumption for the case of maximally entangled particles. (In this sense, our work is related to [23] in the same way as experimental tests of the Bell inequality relate to Bells' theoretical work [4].) Furthermore, we provide a significantly strengthened relation between experimentally measurable quantities and the maximum increase of predictive power any alternative theory could have for these quantities. This allows us to obtain non-trivial bounds on the increased predictive power from experimental data obtained using present technology. In particular, we can falsify all local hidden variable models as well as all (including so far not considered) Leggett-type

models.

Before describing the experiment, we briefly review the main features of the theory (see the Supplemental Material for more details). Crucially, the framework used is operational, i.e., it refers only to directly observable quantities, such as measurement outcomes. For example, the Stern-Gerlach experiment with entangled particles mentioned above outputs a binary value, X (Y), indicating in which direction particle one (two) is deviated. We associate with X (Y) a time coordinate t and three spatial coordinates (r_1, r_2, r_3), corresponding to a point in spacetime where the value X (Y) can be observed. We call such observable values with spacetime coordinates *spacetime variables (SVs)*. In the same manner, any parameters that are needed to specify the experiment (e.g., the orientations of the Stern-Gerlach apparatuses) can be modelled as SVs.

According to quantum theory, the outcome, X, of the measurement on particle one is random, even given a complete description of the measurement apparatus, A. However, an alternative theory may provide us with additional information, Ξ (which can also be modelled in terms of SVs [20]). We can then ask whether this additional information can be used to improve the predictions that quantum mechanics makes about X, which depend on the measurement setting A and the initial state (which we assume to be fixed). This question has a negative answer if the distribution of X, conditioned on A, is unchanged when we learn Ξ. This can be expressed in terms of the Markov chain condition [25],

$$X \leftrightarrow A \leftrightarrow \Xi\,. \tag{1}$$

The aim of this work is to place a bound on the maximum probability, δ, by which this condition can be violated. In other words, a bound of δ implies that the predictions obtained from quantum theory are optimal except with probability (at most) δ.

For the described experiment, the above claim relies only on the natural (and often implicit) assumption that measurement parameters can be chosen freely, i.e., independently of the other parameters of the theory. This assumption can be expressed in the above framework as the requirement that the SV corresponding to a measurement parameter, A, can be chosen such that it is statistically independent of all SVs whose coordinates lie outside the future lightcone of A (Bell's theorem relies on the same assumption, see, e.g., [26]). When interpreted within the usual relativistic spacetime structure, this is equivalent to demanding that A is uncorrelated with any pre-existing values in any frame. We note that any alternative theory that satisfies the free choice assumption automatically obeys the non-signalling conditions, as shown in the Supplemental Material.

As is the case in all falsifications of models that would improve the predictions given by standard quantum theory [4, 13], the argument leading to our bound on δ is based on the strength of correlations between measurement outcomes on entangled particles [27], and, in our case, on pairs of entangled qubits. We denote the projectors describing measurements on qubit one by $|a\rangle\langle a| = \frac{1}{2}(\mathbb{1} + \boldsymbol{S}_A(a)\boldsymbol{\sigma})$ and for qubit two by $|b\rangle\langle b| = \frac{1}{2}(\mathbb{1} + \boldsymbol{S}_B(b)\boldsymbol{\sigma})$ with

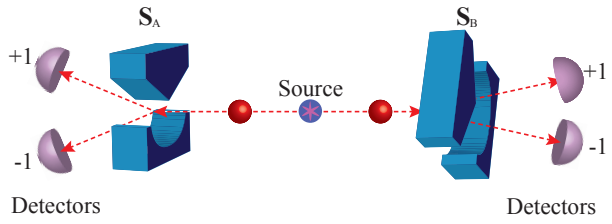


FIG. 3.2.1. A source emits two spin-half particles travelling to two distant sites where each particle's spin is measured along directions $\boldsymbol{S}_A$ and $\boldsymbol{S}_B$, respectively, using Stern-Gerlach apparatuses. If the particles are initially maximally entangled, then the probability of correctly predicting the result of the measurement on the particle on the left ($X = \pm 1$) is, according to quantum mechanics, given by $p_{\mathrm{QM}} = 0.5$.

$$\boldsymbol{S}_A(a) = (\cos(a\pi/2N),\, \sin(a\pi/2N),\, 0)^T$$
$$\boldsymbol{S}_B(b) = (\cos(b\pi/2N),\, \sin(b\pi/2N),\, 0)^T\,,$$

where $a \in \{0, 2, ..., (4N-2)\}$, $b \in \{1, 3, \ldots, (4N-1)\}$, $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)^T$, and ^{T} denotes "transpose". (The spin vectors $\boldsymbol{S}_A(a)$ and $\boldsymbol{S}_B(b)$ are conveniently depicted on the Bloch sphere; Fig. 3.2.3 shows the possible vectors for $N = 3$.) We note that projectors described by values of a (or b) that differ by $2N$ correspond to measurements of spin along opposite directions. Hence, each set of projectors describes N pairs of orthogonal measurements. This allows us to calculate, for each value of $a \in \{0, 2, ..., 2N-2\}$ and $b \in \{1, 3, ..., 2N-1\}$, the probability of detecting the two photons from a pair along the spin directions $\boldsymbol{S}_A(a)$ and $\boldsymbol{S}_B(b)$ (for which we assign $X, Y = +1$), and along the orthogonal directions $-\boldsymbol{S}_A(a)$ and $-\boldsymbol{S}_B(b)$ (for which we assign $X, Y = -1$). We denote this probability $P(X = Y|a, b)$. In turn, this allows us to establish the correlation strength

$$I_N := P(X = Y|0, 2N-1) + \sum_{\substack{a,b \\ |a-b|=1}} (1 - P(X = Y|a, b)). \tag{2}$$

We note that measuring I_N involves the same measurements as those required for testing a chained Bell inequality, first violated for $N \geq 3$ in [28].

Furthermore, deriving a bound on δ requires knowledge of the bias of the individual outcomes

$$\nu_N := \max_a D(P_{X|a}, P_{\bar{X}})\,,$$

where D denotes the variational distance, $D(P_X, Q_X) := \frac{1}{2}\sum_x |P_X(x) - Q_X(x)|$, and $P_{\bar{X}}$ denotes the uniform distribution on X. (In an experiment, due to imperfections in the generated bipartite state that lead to the

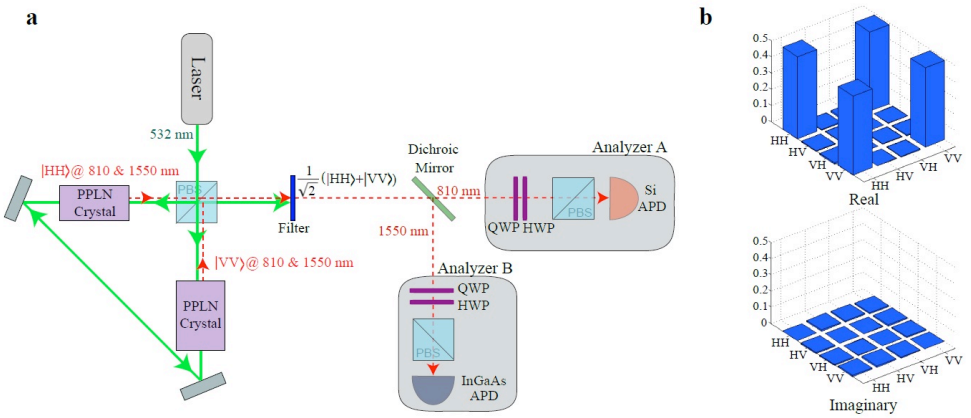


FIG. 3.2.2. (a) Experimental setup, see text for details. (b) Density matrix ρ_{real} of the bi-photon state produced by our source as calculated via maximum-likelihood quantum state tomography [31] (see the Supplemental Material for actual values). The fidelity, $F = \langle\phi^+|\rho_{\text{real}}|\phi^+\rangle$, between the detected state, ρ_{real}, and the ideal state, $|\phi^+\rangle$, given by Eq. 4, is (98.0± 0.1)%).

local (single particle) states not being completely mixed, $P_X(x) \neq 1/2$, which implies a non-zero bias.)

As we show in detail in the Supplemental Material, for each N, the maximum increase of predictive power, δ_N, of any alternative theory is bounded by

$$\delta_N = \frac{I_N}{2} + \nu_N. \tag{3}$$

Repeating the correlation and bias measurements for many N, we can obtain the best bound on δ via $\delta \leq \min_N\{\delta_N\}$. Assuming a perfect experimental setup, quantum theory predicts that δ_N will approach 0 as N tends to ∞. For a realistic (imperfect) setup, however, δ_N reaches a minimum at some finite N, above which it is increasing in N.

A schematic of our experimental setup [29], which is inspired by the source described in [30], is depicted in Fig. 3.2.2. A diagonally polarized, continuous wave, 532 nm wavelength laser beam is split by a polarizing beam splitter (PBS) and travels both clockwise and counter-clockwise through a polarization Sagnac interferometer. The interferometer contains two type-I, periodically poled lithium niobate (PPLN) crystals configured to produce collinear, non-degenerate, 810/1550 nm wavelength photon pairs via spontaneous parametric down-conversion. As the optical axes of the two crystals are perpendicular to each other and photon-pair generation is polarization dependent, the clockwise-travelling, vertically polarized (counter-clockwise travelling, horizontally polarized) pump light passes through the first crystal without interaction and may down-convert in the second crystal to produce two horizontally (vertically) polarized photons. For small pump power, recombination of the two bi-photon modes on the PBS yields photon pairs with high fidelity to the maximally entangled state

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle), \tag{4}$$

where $|H\rangle$ and $|V\rangle$ represent horizontal and vertical polarization states, respectively, and replace the usual spin-up and spin-down notation for spin-half particles. Behind the interferometer, the remaining pump light is removed using a high-pass filter. The entangled photons are separated on a dichroic mirror and sent to polarization analyzers that can be adjusted to measure the polarization of an incoming photon along any desired direction $\boldsymbol{S} = (S_H, S_+, S_L)^T$, where $\boldsymbol{S}$ is expressed in terms of its projections onto horizontal (H), diagonal (+45°), and left-circular (L) polarized components. The polarization analyzers consist of quarter wave plates (QWP), half wave plates (HWP), and PBSs. Finally, the 810 nm photons are detected using a free-running Silicon avalanche photo-diode (Si APD), and 1550 nm photons are detected using an InGaAs APD triggered by detection events from the Si APD.

For each setting $\boldsymbol{S}_A(a)$ (with a as described above), we establish the number of detected photons, $M(a)$, over 80 sec, from which we can calculate the bias

$$\nu_N = \frac{1}{2} \max_{a\in\{0,2,\ldots,(2N-2)\}} \left\{ \frac{|M(a) - M(a+2N)|}{M(a) + M(a+2N)} \right\}.$$

Furthermore, for the joint measurements described by Eq. 2, we register the number of detected photon pairs over 40 sec to calculate

$$P(X = Y|a,b) = \frac{M(a,b) + M(a+2N, b+2N)}{M},$$

where, e.g., $M(a,b)$ is the number of joint photon detections for measurements along $\boldsymbol{S}_A(a)$ and $\boldsymbol{S}_B(b)$, and

N	I_N	ν_N	δ_N
2	0.6213 ± 0.0035	0.0025 ± 0.0002	0.3131 ± 0.0018
3	0.4549 ± 0.0032	0.0020 ± 0.0002	0.2294 ± 0.0016
4	0.3757 ± 0.0029	0.0025 ± 0.0002	0.1904 ± 0.0015
5	0.3518 ± 0.0028	0.0033 ± 0.0002	0.1792 ± 0.0014
6	0.3290 ± 0.0028	0.0032 ± 0.0002	0.1677 ± 0.0014
7	0.3238 ± 0.0027	0.0025 ± 0.0002	0.1644 ± 0.0014

TABLE 3.2.1. Summary of Results. The table shows values for I_N, bias ν_N, as well as $\delta_N = I_N/2 + \nu_N$. Statistical uncertainties (one standard deviation) are calculated from measurement results assuming Poissonian statistics.

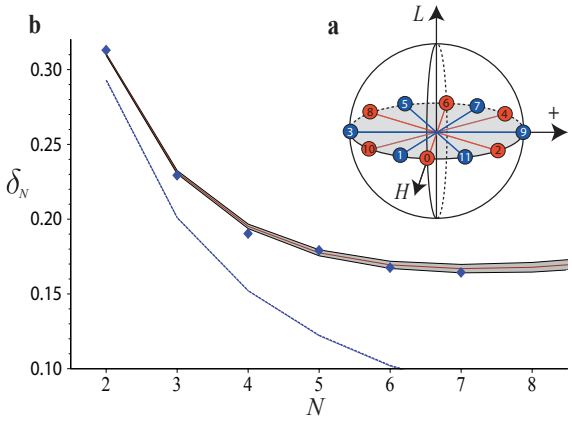


FIG. 3.2.3. (a) Measurement settings. Graphical depiction of the polarization measurements along $\boldsymbol{S}_A$ (red, labelled using index A, i.e. even numbers) and $\boldsymbol{S}_B$ (blue, labelled using index B, i.e. odd numbers) for $N = 3$. (b) Results. Experimentally obtained values δ_N (blue diamonds) with one-standard-deviation uncertainties (hidden by the size of the diamonds) calculated from measurement results assuming Poissonian statistics. Also shown is a curve joining the values predicted by quantum theory, including one-standard-deviation statistical uncertainties (solid red line and grey shaded area, respectively), calculated from the measured density matrix ρ_{real}. Note that the predicted value for δ increases for $N > 7$. The bounds of the shaded region are derived using Monte Carlo simulations and are consistent with the observed variations of the measured values. Finally, the dashed blue line is the theoretical curve, again calculated using quantum theory, that assumes the ideal $|\phi^+\rangle$ state, as in Eq. 4, and perfect experimental apparatus with zero noise. It asymptotically approaches zero as N tends to infinity. For instance, for $N = 7$ we find $\delta_7^{\text{ideal}} = 0.088$.

the normalization factor $M = M(a, b) + M(a, b + 2N) + M(a + 2N, b) + M(a + 2N, b + 2N)$. This allows us to establish δ_N via Eqs. 2 and 3.

Our experimental results are depicted in Fig. 3.2.3 and summarized in Table 3.2.1. We measured δ_N for $N = 2$ to $N = 7$ and found the minimum, $\delta_7 = 0.1644 \pm 0.0014$, for $N = 7$. Using the above considerations, these data lead to our main conclusion that the maximum probability by which any alternative theory can improve the predictions of quantum theory is at most $\sim$0.165. To put this result into context, we note that a deterministic local hidden variable theory would allow for predictions of the outcomes with probability $p_{LHV} = 1$; similarly, it is easy to verify that the Leggett model (with a uniform distribution over the hidden spin, z) would correctly predict the outcome with probability $p_{Leggett} = 3/4$. Since these values exceed $p_{QM} = 1/2$ by more than delta, both theories are directly falsified by our result. (We refer to the Supplemental Material for a more detailed discussion of the Leggett model, including variants with a different distribution of the hidden spin vector.) We remark that our conclusion is based on the assumption that measurement settings can be chosen freely (this removes the necessity to experimentally close the locality loophole), and our experiments do not close the detection loophole [10]. Hence, strictly, the above conclusion holds modulo the assumption that similar, loophole-free experiments would show the same results.

Further decreasing the experimentally established bound on δ would require photon pair sources and measurement apparatuses with rapidly increasing quality. For example, to decrease δ by more than a factor of two compared to our result, the fidelity must exceed 99.6% (assuming zero bias and perfect measurement apparatus) and N increases to 15 or beyond, resulting in 120 or more high-precision coincidence measurements. This is, to the best of our knowledge, unattainable with state-of-the-art sources [16, 17] (for more details see the Supplemental Material).

In conclusion, under the assumption that measurements can be chosen freely, no theory can predict the outcomes of measurements on a member of a maximally entangled pair substantially better than quantum mechanics. In other words, any already considered or yet-to-be-proposed theory that makes significantly better predictions would either be incompatible with our experimental observations, or be incompatible with our assumption that the measurement parameters can be chosen freely. While the former is true, for example, for local hidden variable theories (as already pointed out by Bell [4]) or for the Leggett model [13], the de Broglie-Bohm theory [32, 33] is an example of the second type – the theory cannot incorporate measurement parameters that satisfy our free-choice assumption (this is further discussed in the Supplemental Material).

ACKNOWLEDGEMENTS

The authors thank F. Bussières for help with setting up the photon pair source, and V. Kiselyov for technical support. Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation. R.R. acknowledges support

from the Swiss National Science Foundation (grant No. 200020-135048 and the NCCR QSIT) and from the European Research Council (grant No. 258932). W.T., T.E.S. and J.A.S. are supported by NSERC, QuantumWorks, General Dynamics Canada, iCORE (now part of Alberta Innovates Technology Futures), CFI and AAET.

[1] A. Einstein, B. Podolsky, B. and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47**, 777–780 (1935).

[2] S. Kochen and E. P. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics* **17**, 59–87 (1967).

[3] J. S. Bell. On the problem of hidden variables in quantum mechanics. *Rev. Modern Physics* **38**, 447–452 (1966).

[4] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics* **1**, 195–200 (1964).

[5] S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.* **28**, 938–941 (1972).

[6] A. Aspect, P. Grangier and G. Roger. Experimental realization of Einstein-Podolsky-Rosen-Bohm gedankenexperiment: A new violation of Bell's inequalities. *Phys. Rev. Lett.* **49**, 91–94 (1982).

[7] W. Tittel *et al.* Experimental demonstration of quantum correlations over more than 10 km. *Phys. Rev. A* **57**, 3229–3232 (1998).

[8] G. Weihs *et al.* Violation of Bell's inequality under strict Einstein locality conditions. *Phys. Rev. Lett.* **81**, 5039–5043 (1998).

[9] M. A. Rowe *et al.* Experimental violation of a Bell's inequality with efficient detection. *Nature* **409**, 791–794 (2001).

[10] A. Aspect. Bell's inequality test: More ideal than ever. *Nature* **398**, 189–190 (1999).

[11] In his later works, Bell uses definitions that potentially allow probabilistic models [12]. However, as explained in the Supplementary Information of [20], non-deterministic models are not compatible with Bell's other assumptions.

[12] J. S. Bell. La nouvelle cuisine. In *Between Science and Technology*, chap. 24, 97–115, Elsevier Science Publishers, (1990).

[13] A. J. Leggett. Nonlocal hidden-variable theories and quantum mechanics: An incompatibility theorem. *Foundations of Physics* **33**, 1469–1493 (2003).

[14] More details, as well as other distributions are discussed in the Supplemental Material.

[15] S. Gröblacher *et al.* An experimental test of non-local realism. *Nature* **446**, 871–875 (2007).

[16] T. Paterek *et al.* Experimental test of nonlocal realistic theories without the rotational symmetry assumption. *Phys. Rev. Lett.* **99**, 210406 (2007).

[17] C. Branciard *et al.* Experimental falsification of Leggett's non-local variable model. *Phys. Rev. Lett.* **99**, 210407 (2007).

[18] M. D. Eisaman *et al.* Experimental test of nonlocal realism using a fiber-based source of polarization-entangled photon pairs. *Phys. Rev. A* **77**, 032339 (2008).

[19] C. Branciard *et al.* Testing quantum correlations versus single-particle properties within Leggett's model and beyond. *Nat. Phys.* **4**, 681–685 (2008).

[20] R. Colbeck and R. Renner. No extension of quantum theory can have improved predictive power. *Nat. Commun.* **2**, 411 (2011).

[21] J. Barrett, L. Hardy and A. Kent. No signalling and quantum key distribution. *Phys. Rev. Lett.* **95**, 010503 (2005).

[22] J. Barrett, A. Kent and S. Pironio. Maximally non-local and monogamous quantum correlations. *Phys. Rev. Lett.* **97**, 170409 (2006).

[23] R. Colbeck and R. Renner. Hidden variable models for quantum theory cannot have any local part. *Phys. Rev. Lett.* **101**, 050403 (2008).

[24] More precisely, the assumption that quantum theory is correct was divided into two parts, the first being that a particular experimental setup yields outcomes distributed as predicted by the theory, and the second that measurement processes can be considered as unitary operations if one takes into account the environment. Here we experimentally investigate the first assumption. Note that the second assumption is only required when bounding the predictive power for measurements on particles that are not members of maximally entangled pairs.

[25] T. M. Cover and J. A. Thomas. *Elements of Information Theory* (John Wiley and Sons Inc., 2006), 2nd edn. Section 2.8.

[26] J. S. Bell. Free variables and local causality. *Epistemological Letters* **38**, (1977).

[27] Considering measurements restricted to single particles always leaves open the possibility of explaining the results using a local hidden variable model, see Appendix I.

[28] E. Pomarico *et al.* Various quantum nonlocality tests with a commercial two-photon entanglement source. *Phys. Rev. A* **83**, 052104 (2011).

[29] T. E. Stuart, J. A. Slater, F. Bussières and W. Tittel. In preparation.

[30] T. Kim *et al.* Fiorentino, M.& Wong, F. N. C. Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer. *Phys. Rev. A* **73**, 12316 (2006).

[31] J. B. Altepeter, E. R. Jeffrey and P. G. Kwiat . Photonic state tomography. *Advanced Atomic and Optical Physics* **52**, 105–159 (2005).

[32] L. de Broglie. La mécanique ondulatoire et la structure atomique de la matire et du rayonnement. *Journal de Physique, Serie VI* **VIII**, 225–241 (1927).

[33] D. Bohm. A suggested interpretation of the quantum theory in terms of "hidden" variables. I. *Phys. Rev.* **85**, 166–179 (1952).

Chapter 4

Quantum Entanglement for Quantum Cryptography

Quantum entanglement gives rise to correlations that are fundamentally different from correlations possible in a local realistic world. In the previous chapter we have tested those differences in a variety of ways, which, in turn, allows us to confirm our ability to produce high-fidelity entanglement. Entanglement can then be used for many practical applications, such as QKD.

The security of QKD has been proven under various assumptions about the devices of the legitimate QKD players, Alice and Bob. While commercial and high-performance research systems exist, the next-generation of QKD research is moving towards understanding potential side-channels and closing them with effective counter-measures. For our research into next-generation systems, we chose to study and implement a new protocol known as MDI-QKD [47].

In previously-developed entanglement-based protocols [5, 37], a source of entanglement is stationed between Alice and Bob that sends one qubit to Alice and one qubit to Bob, who both perform projection measurements (see Chapter 1). In contrast to this, and prepare-and-measure QKD, in MDI-QKD Alice and Bob both generate single qubits in one of four states and send these to a third-party named Charlie. Charlie performs a BSM with the qubits he receives and then informs Alice and Bob which qubits projected onto which Bell state. Charlie's only purpose is to essentially create entanglement between Alice and Bob, which, as he is the only participant using detectors and performing measurements, closes all possible detector side-channels in the process. In particular, not even Charlie himself can gain information about the key without introducing detectable errors.

The motivation for choosing this protocol was three-fold. First, it is an example of the

use of entanglement to provably close side-channels, which is an important goal in next-generation QKD research. Second, Charlie's BSM is between photons generated by independent sources that have travelled through independent channels and this had not been demonstrated previously. This is also a necessary feat for quantum repeaters and so we believe that the techniques we developed for MDI-QKD will be useful for future repeater experiments. Finally, MDI-QKD seems well suited for networked QKD. Generally QKD is performed over point-to-point links between only two individuals and there is some research push to develop networked QKD systems. With MDI-QKD one could envision Charlie at the centre of a network with fibres connecting him to a many Alices and Bobs (the so-called *star* network), whom he "connects", like a switchboard, by entangling their photons. Charlie could also be connected to a larger, high-rate, long-distance network and act as a hub connecting the nearby Alices and Bobs to the larger network. As Charlie is the only participant performing measurements and as detector technology is generally more expensive and more difficult to run, this network design minimizes costs be keeping expensive technology all in a single place, while cheap, easy-to-use sources are with scattered end users.

This chapter contains two articles. In the first paper we developed our experimental QKD system as well as a general, detailed, theoretical model of the performance of MDI-QKD systems. The model contains parameters describing identifiable imperfection in any system, and can be used to predict experimentally measurable quantities, such as error rates and secret key rates. We deployed our system across the city of Calgary and we found very good agreement between our theoretical model and measurement results. The purpose of the model was to understand how to optimize secret key generation rates and to learn what imperfections limit secret key generation rates. Since our demonstration, two other groups have demonstrated MDI-QKD [70, 71] and our hope is that they and future researchers will use this model to optimize their systems as well.

In the second article, we added an MDI-QKD decoy-state protocol to our implementation

to protect against PNS attacks (as described in Chapter 1) and again deployed across the city of Calgary. This proof-of-principle demonstration proved the feasibility of both MDI-QKD and real-world BSMs, as needed for quantum repeaters and a host of other quantum communication applications.

This work was done in collaboration with Allison Rubenok and the QC2 cryptography team. I contributed to these studies in the following stages: I worked on developing the system, developing the model, performing the measurements, and analyzing the results.

Modeling a Measurement-Device-Independent Quantum Key Distribution System

P. Chan[1,2], J. A. Slater[1,3], I. Lucio-Martinez[1,3], A. Rubenok[1,3], W. Tittel[1,3]

[1]Institute for Quantum Science & Technology, University of Calgary, 2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada.
[2]Department of Electrical & Computer Engineering, University of Calgary, 2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada.
[3]Department of Physics & Astronomy, University of Calgary, 2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada.

Abstract. We present a detailed description of a widely applicable model for quantum key distribution (QKD) systems implementing the measurement-device-independent (MDI) protocol. The validity of the model is confirmed by comparing its predictions with real-world data taken using a time-bin qubit-based QKD system in various configurations. This allows using the model to optimize mean photon numbers per attenuated laser pulse, which are used to encode quantum bits. In turn, this allows optimizing secret key rates of existing MDI-QKD systems, identifying rate-limiting components, and projecting future performance.

1. Introduction

From the first proposal in 1984 to now, the field of quantum key distribution (QKD) has evolved significantly [1, 2]. For instance, experimentally, systems delivering key at Mbps rates [3] as well as key distribution over more than 100 km [4, 5] have been reported. From a theoretical perspective, efforts aim at developing QKD protocols and security proofs with minimal assumptions about the devices used [6]. Of particular practical importance are two recently developed protocols that do not require trusted single photon detectors (SPDs) [7, 8]. One of these, the so-called measurement-device-independent QKD (MDI-QKD) protocol, has already been implemented experimentally [9, 10, 11]. Hence, it is foreseeable that it will play an important role in the future of QKD, and it is thus important to understand the interplay between experimental imperfections (which will always remain in real systems) and system performance to maximize the latter.

In this work, we present a detailed description of a widely applicable mathematical model describing systems that implement the MDI-QKD protocol. The model takes into account imperfect state preparation, loss in the quantum channel, as well as limited detector efficiency and noise. The validity of our model is assessed by comparing its

predictions with real-world data taken with an MDI-QKD system employing time-bin qubits [9]. Our system is used in two different configurations: In the first configuration, all parties required for key distribution are situated within the same laboratory and are connected through spooled fibers of different lengths, while in the second, the protocol is performed over deployed fiber across the city of Calgary (see Fig. 4.1.1 for a schematics). Our model reproduces the experimental data within statistical uncertainties, regardless of whether experiments were performed using spooled or deployed fibers. In turn, this validation allows optimizing central parameters that determine secret key rates, such as mean photon numbers used to encode qubits, and to identify rate-limiting components for future system improvement.

This paper is organized in the following way: In section 2 we detail some of the side-channel attacks (i.e. attacks exploiting incorrect assumptions about the working of QKD devices) proposed so far and review technological countermeasures. In section 3 we briefly describe the MDI-QKD protocol, which instead exploits fundamental quantum physical laws to render the most important of these attacks useless. Our model of MDI-QKD systems is presented in section 4. This section is followed by an in-depth account of experimental imperfections that affect MDI-QKD performance and a description of how we characterized them in our system (section 5). Section 6 shows the results of the comparison between modelled and measured quantities, and section 7 details how to optimize the performance of our MDI-QKD system using the model. Finally, we conclude the article in section 8.

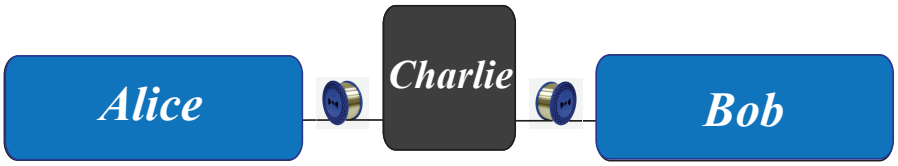


Figure 4.1.1. Schematics for MDI-QKD. Charlie facilitates the key distribution between Alice and Bob without being able to learn the secret key.

2. Side-channel attacks

A healthy development of QKD requires investigating the vulnerabilities of QKD implementations in terms of potential side-channel attacks. Side-channels in QKD are channels over which information about the key may leak out unintentionally. One of the first QKD side-channel attacks proposed was the photon number splitting (PNS) attack [12] in which the eavesdropper, Eve, exploits the fact that attenuated laser pulses sometimes include more than one photon to obtain information about the key. This attack can be detected if the decoy state protocol [13, 14, 15] is implemented. In the decoy state protocol, Alice varies the mean photon number per pulse in order to allow her and Bob to distill the secret key only from information stemming from single photon

emissions. More proposals of side-channel attacks followed, including the Trojan-horse attack [16], for which the countermeasure is an optical isolator [16], and the phase remapping attack [17], for which the countermeasure is phase randomization [17]. Later on, attacks that took advantage of SPD vulnerabilities were also proposed [18, 19, 20, 21]. For example, the time-shift attack [19] exploits a difference in the quantum efficiencies of the SPDs used in a QKD system. This attack can be prevented by actively selecting one of the two bases for the projection measurement, as well as by monitoring the temporal distribution of photon detections [19]. Another example is the detector blinding attack [21] in which the eavesdropper uses high intensity pulses to modify the performance (i.e. blind) the SPDs. Due to its power, it is currently of particular concern. The blinding attack can be detected by monitoring the intensity of light at the entrance of Bob's devices with a photodiode [21, 22, 23].

It is important to mention that open side-channels do not necessarily compromise the security of the final key if the information that Eve may have obtained through an attack is properly removed during privacy amplification. However, as technological fixes (as discussed above) or additional privacy amplification can only thwart known attacks, it is important to develop and implement protocols that use a minimum number of assumptions about the devices used to implement the protocol. An important example is the measurement-device-independent QKD protocol, which we will introduce in the next section.

3. The Measurement-Device-Independent Quantum Key Distribution Protocol

The MDI-QKD protocol is a time-reversed version of entanglement-based QKD. In this protocol, the users, Alice and Bob are each connected to Charlie, a third party, through a quantum channel, e.g. optical fiber (see Fig. 4.1.1). In the ideal version, the users have a source of single photons that they prepare randomly in the BB84 qubit states [24] $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$, where $|\pm\rangle = 2^{-1/2}(|0\rangle \pm |1\rangle)$. The qubits are sent to Charlie where the SPDs are located. Charlie performs a partial Bell state measurement (BSM) through a 50/50 beam splitter and then announces the events for which the measurement resulted in a projection onto the $|\psi^-\rangle = 2^{-1/2}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$ state. Alice and Bob then publicly exchange information about the basis (z, spanned by $|0\rangle$ and $|1\rangle$, or x, spanned by $|+\rangle$ and $|-\rangle$. Associating quantum states with classical bits (e.g. $|0\rangle, |-\rangle \equiv 0$, and $|1\rangle, |+\rangle \equiv 1$) and keeping only events in which Charlie found $|\psi^-\rangle$ and they picked the same basis, Alice and Bob now establish anti-correlated key strings. (Note that a projection of two photons onto $|\psi^-\rangle$ indicates that the two photons, if prepared in the same basis, must have been in orthogonal states.) Bob then flips all his bits, thereby converting the anti-correlated strings into correlated ones. Next, the so-called *x-key* is formed out of all key bits for which Alice and Bob prepared their photons in the x-basis; its error rate is used to bound the information an eavesdropper may have acquired during photon transmission. Furthermore, Alice and Bob form the *z-key* out of those

bits for which both picked the z-basis. Finally, they perform error correction and privacy amplification[1, 2] to the *z-key*, which results in the secret key.

The advantage of MDI-QKD protocol over conventional prepare-and-measure or entangled photon-based QKD protocols is that detection events are uncorrelated with the final secret key bits. This is because a projection onto $|\psi^-\rangle$ only indicates that Alice and Bob sent anti-correlated states, but does not reveal who sent which state. As a result, Eve (including a dishonest Charlie) is unable to gain any information about the key from passively monitoring the detectors or implementing a detector side-channel attack. In fact, all detector side channels are closed in MDI-QKD.

Note that the ideal version of MDI-QKD protocol assumes that Charlie performs a perfect partial BSM. While this is required to maximize the secret key rate, it is not necessary to guarantee security of the key. Indeed, the key distribution is not compromised if the measurement is different, regardless wether the difference is due to experimental imperfections, or to an eavesdropper (including Charlie) trying to gather information about the states that Alice and Bob sent. An imperfect BSM will simply result in a higher error rate and thus to a smaller secret key rate once error correction and privacy amplification have been applied.

In the ideal scenario introduced above, Alice and Bob use single photon sources to generate qubits. However, it is possible to implement the protocol using light pulses attenuated to the single photon level. Indeed, as in prepare-and-measure QKD, randomly varying the mean photon number of photons per attenuated light pulse between a few different values (so-called decoy and signal states) allows making the protocol practical while protecting against a possible PNS attack [7, 25]. The secret key rate is then given by [7]:

$$S = Q_{11}^z(1 - h_2(e_{11}^x)) - Q_{\mu\sigma}^z f h_2(e_{\mu\sigma}^z), \tag{1}$$

where h_2 is the binary entropy function, f indicates the error correction efficiency, Q indicates the gain (the probability of a projection onto $|\psi^-\rangle$ per emitted pair of pulses) and e indicates error rates (the ratio of erroneous to total projections onto $|\psi^-\rangle$). Furthermore, the superscripts, x or z, denote if gains or error rates are calculated for qubits prepared in the x- or the z-basis, respectively. Similarly, the subscripts, μ and σ, show that the quantity under concern is calculated or measured for pulses with mean photon number μ (sent by Alice) and σ (sent by Bob), respectively. Finally, the subscript 11 indicates quantities stemming from events for which the pulses emitted by Alice and Bob contain only one photon each. Note that Q_{11} and e_{11} cannot be measured; their values must be bounded using a decoy state method.

Shortly after the original proposal [7], a practical decoy state protocol for MDI-QKD was proposed in [25]. It requires Alice and Bob to randomly pick mean photon numbers between two decoy states and a signal state. One of the decoy states must have a mean photon number lower than the signal state, while the other one must be vacuum. A finite number of decoy states results in a lower bound for $Q_{11}^{x,z}$ and an upper

bound for e_{11}^x, which in turn gives a lower bound for the secret key rate in Eq. 1. We will elaborate more on decoy states in section 7.1.

4. The Model

4.1. Assumptions

The four main assumptions or approximations under which our model has been developed are the following:

- We assume the sources located at Alice and Bob, respectively, generate phase randomized mixtures of photon number states (Fock states) with known distribution $\mathbb{D}(\ltimes)$ (e.g. Poissonian or thermal distribution, etc).
- After Charlie's beam splitter, we consider terms of up to three photons only. Considering higher-order terms would slightly raise the gains and error rates predicted by the model. However, given the low average photon numbers and the typical channel loss in real-world quantum channels, this effect is negligible.
- Charlie's beam splitter is a perfect 50/50, lossless beam splitter. A deviation from this approximation does not open a security loophole as an imperfect beam splitter implies that Charlie's measurement is an imperfect Bell state measurement, which increases the error rates measured by Alice and Bob. Effectively, this degrades the (entangled) channel between Alice and Bob, which results in a decreased secret key rate.
- Charlie's two single-photon detectors have identical properties. We note that a deviation from this approximation also does not open a potential security loophole (in contrast to prepare-and-measure and entangled photon based QKD), as all detector side-channel attacks are removed in MDI-QKD.

4.2. Derivation of the model

Our model takes into account imperfections present in a typical QKD system. Regarding the sources, located at Alice and Bob, we take into account imperfect preparation of the quantum state of each photon. Furthermore, we consider transmission loss of the links between Alice and Charlie and Bob and Charlie. And finally, concerning the measurement apparatus at Charlie's, we consider imperfect projection measurement stemming from non-maximum quantum interference on Charlie's beam splitter, detector noise such as dark counts and afterpulsing, and limited detector efficiency.

In the following paragraphs we present a detailed description of our model. We note that, in order to facilitate explanations, we have adopted the terminology of time-bin encoding. However, our model is general and can also be applied to MDI-QKD systems implementing any kind of encoding.

4.2.1. State preparation In the MDI-QKD protocol, Alice and Bob derive key bits whenever Charlie announces a projection onto the $|\psi^-\rangle$ Bell state. We model the probability of a $|\psi^-\rangle$ projection for various quantum states of photons emitted by Alice and Bob‡ as a function of the mean photon number per pulse (μ and σ respectively) and transmission coefficients of the fiber links (t_A and t_B, respectively)§. We consider qubit states described by:

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

where $|0\rangle$ and $|1\rangle$ denote photons in orthogonal modes (i.e. early and late temporal modes assuming time-bin qubits), respectively. Note that $|\psi\rangle$ describes any pure state. In the ideal case, $m^z \in [0, 1]$ for photon preparation in the z-basis (in this case, the value of ϕ^z is irrelevant), $m^x = \frac{1}{2}$ and $\phi^x \in [0, \pi]$ for the x-basis, and $b^{x,z} = 0$ for both bases. Imperfect preparation of photon states is modelled by using non-ideal $m^{x,z}$, $\phi^{x,z}$ and $b^{x,z}$ for Alice and Bob. The parameter $b^{x,z}$ is included to represent the background light emitted by an imperfect source‖. Furthermore, in principle, the various states generated by Alice and Bob could have differences in other degrees of freedom (i.e. polarization, spectral, spatial, temporal modes). This is not included into Eq. 2.

4.2.2. Conditional probability for projections onto $|\psi^-\rangle$ A projection onto $|\psi^-\rangle$ occurs if one of the SPDs behind Charlie's 50/50 beam splitter signals a detection in an early time-bin (a narrow time interval centered on the arrival time of photons occupying an early temporal mode) and the other detector signals a detection in a late time-bin (a narrow time-interval centered on the arrival time of photons occupying a late temporal mode). Note that, in the following paragraphs, this is the desired detection pattern we search for when modelling possible interference cases or noise effects.

We build up the model by first considering the probabilities that particular outputs from the beam splitter (at Charlie's) will generate the detection pattern associated with a projection onto $|\psi^-\rangle$. The outputs are characterized by the number of photons per output port as well as their quantum state. The probabilities for each of the possible outputs to occur can then be calculated based on the inputs to the beam splitter (characterized by the number of photons per input port and their quantum states, as defined in Eq. 2). Note that for the simple cases of inputs containing zero or one photon (summed over both input modes), we calculate the probabilities leading to the desired detection pattern directly, i.e. without going through the intermediate step of calculating outputs from the beam splitter. Finally, the probability for each input to occur is calculated based on the probability for Alice and Bob to send attenuated light pulses containing exactly i photons, all in a state given by Eq. 2. The probability for a particular input to occur also depends on the transmissions of the quantum channels,

‡ Note that all photons within a specific attenuated light pulse are in the same quantum state.
§ Normally t is given by the optical loss in the fiber. However, if modelling eavesdropping, t might be photon number dependent.
‖ Note how the added background leads to non-normalized states.

t_A and t_B. We recall that this model considers up to three photons incident on the beam splitter. This is sufficient as, in the case of heavily attenuated light pulses and lossy transmission, higher order terms do not contribute significantly to projections onto $|\psi^-\rangle$. However, we limit the following description to two photons at most: the extension to three is straightforward and follows the methodology presented for two photons.

Detector noise Let us begin by considering the simplest case in which no photons are input into the beam splitter. In this case, detection events can only be caused by detector noise. We denote the probability that a detector indicates a spurious detection as P_n. Detector noise stems from two effects: dark counts and afterpulsing [26]. Dark counts represent the base level of noise in the absence of any light, and we denote the probability that a detector generates a dark count per time-bin as P_d. Afterpulsing is an additional noise source produced by the detector as a result of prior detection events. The probability of afterpulsing depends on the total count rate, hence we denote the afterpulsing probability per time-bin as P_a, which is a function of the mean photon number per pulse from Alice and Bob (μ and σ), the transmission of the channels (t_A and t_B) and the efficiency of the detectors (η) located at Charlie (see below for afterpulse characterization). The total probability of a noise count in a particular time-bin is thus $P_n = P_d + P_a$. All together, we find the probability (conditioned on having no photons input into the beam splitter) for generating the detection pattern associated with a projection onto the $|\psi^-\rangle$-state to be:

$$P(|\psi^-\rangle|0 \text{ photons, in}) = P(|\psi^-\rangle|0 \text{ photons, out}) = 2P_n^2, \tag{3}$$

Here and henceforward, we have ignored the multiplication factor (1-P_n) ~ 1¶, which indicates the probability that a noise event did not occur in the early time-bin (this is required in order to see a detection during the late time-bin assuming detectors with recovery time larger than the separation between the $|0\rangle$ and $|1\rangle$ temporal modes). Note that the probability conditioned on having no photons at the inputs of the beam splitter equals the one conditioned on having no photons at the outputs.

One-photon case Next, we consider the case in which a single photon arrives at the beam splitter. To generate the detection pattern associated with $|\psi^-\rangle$, either the photon must be detected and a noise event must occur in the other detector in the opposite time-bin, or, if the photon is not detected, two noise counts must occur as in Eq. 3. We find

$$P(|\psi^-\rangle|1 \text{ photon, in}) = \eta P_n + (1-\eta)P(|\psi^-\rangle|0 \text{ photons, out}), \tag{4}$$

where η denotes the probability to detect a photon that occupies an early (late) temporal mode during an early (late) time-bin (we assume η to be the same for both detectors).

¶ Note that this approximation is, in general, not required. However, in order to obtain the best performance from a QKD implementation, the noise level should be as low as possible, i.e. $P_n \sim 0$.

Two-photon case We now consider detection events stemming from two photons entering the beam splitter. The possible outputs can be broken down into three cases. In the first case, both photons exit the beam splitter in the same output port and are directed to the same detector. This yields only a single detection event, even if the photons are in different temporal modes. The probability for Charlie to declare a projection onto $|\psi^-\rangle$ is then

$$\begin{aligned} &P(|\psi^-\rangle|2 \text{ photons, 1 spatial mode, out}) = \\ &\quad (1-(1-\eta)^2)P_n + (1-\eta)^2 P(|\psi^-\rangle|0 \text{ photons, out}). \end{aligned} \tag{5}$$

In the second case, the photons are directed towards different detectors and occupy the same temporal mode. Hence, to find detections in opposite time-bins in the two detectors, at least one photon must not be detected. This leads to

$$\begin{aligned} &P(|\psi^-\rangle|2 \text{ photons, 2 spatial modes, 1 temporal mode, out}) = \\ &\quad 2\eta(1-\eta)P_n + (1-\eta)^2 P(|\psi^-\rangle|0 \text{ photons, out}). \end{aligned} \tag{6}$$

In the final case, both photons occupy different spatial as well as temporal modes. In contrast to the previous case, a projection onto $|\psi^-\rangle$ can now also originate from the detection of both photons. This leads to

$$\begin{aligned} &P(|\psi^-\rangle|2 \text{ photons, 2 spatial modes, 2 temporal modes, out}) = \\ &\quad \eta^2 + 2\eta(1-\eta)P_n + (1-\eta)^2 P(|\psi^-\rangle|0 \text{ photons, out}). \end{aligned} \tag{7}$$

In order to find the probability for each of the three two-photon outputs to occur, we now examine two-photon inputs to the beam splitter. For ease of analysis, we first introduce some notation:

$$\begin{aligned} p^{x,z}(0,0) &\equiv (m_1^{x,z} + b_1^{x,z})(m_2^{x,z} + b_2^{x,z}) \\ p^{x,z}(0,1) &\equiv (m_1^{x,z} + b_1^{x,z})(1 - m_2^{x,z} + b_2^{x,z}) \\ p^{x,z}(1,0) &\equiv (1 - m_1^{x,z} + b_1^{x,z})(m_2^{x,z} + b_2^{x,z}) \\ p^{x,z}(1,1) &\equiv (1 - m_1^{x,z} + b_1^{x,z})(1 - m_2^{x,z} + b_2^{x,z}) \\ b_{norm}^{x,z} &\equiv 1 + 2b_1^{x,z} + 2b_2^{x,z} + 4b_1^{x,z} b_2^{x,z} \end{aligned} \tag{8}$$

where $b_{1,2}^{x,z}$ and $m_{1,2}^{x,z}$ are the parameters introduced in Eq. 2; the subscripts label the photon (one or two) whose state is specified by the parameters. Furthermore, $p^{x,z}(i,j)$ is proportional to finding photon one in temporal mode i and photon two in temporal mode j, where $i, j \in [0,1]$. Finally, $b_{norm}^{x,z}$ is a normalization factor.

We note that it is possible for the two photons to be subject to a two-photon interference effect (known as photon bunching) when impinging on the beam splitter.

Let us first consider the case in which the two photons do not interfere. This case occurs if both photons either come from the same source, or if they come from different sources and are perfectly distinguishable (for example, if they had orthogonal polarizations). With probability 1/2 the two photons exit the beam splitter in the same output port (or spatial mode). Furthermore, with probability $A = [p^{x,z}(0,0) + p^{x,z}(1,1)]/2b^{x,z}_{\text{norm}}$ we find the photons in different spatial modes and in the same temporal mode, and with probability $B = [p^{x,z}(0,1) + p^{x,z}(1,0)]/2b^{x,z}_{\text{norm}}$ we find the photons in different spatial and temporal modes. Thus the probability that Charlie finds the desired detection pattern is:

$$\begin{aligned} &P(|\psi^-\rangle|2 \text{ photons, non-interfering, in}) = \\ &\quad \frac{1}{2} P(|\psi^-\rangle|2 \text{ photons, 1 spatial mode, out}) \\ &\quad + A \times P(|\psi^-\rangle|2 \text{ photons, 2 spatial modes, 1 temporal mode, out}) \\ &\quad + B \times P(|\psi^-\rangle|2 \text{ photons, 2 spatial modes, 2 temporal modes, out}). \end{aligned} \tag{9}$$

Finally, consider the case in which the two input photons interfere on the beam splitter, which occurs if they come from different sources and are indistinguishable. In this case, the probabilities of finding the outputs from the beam splitter discussed in Eqs. 5-7 are dependent on the phase difference between the states of the two photons, $\Delta\phi^{x,z} \equiv \phi_1^{x,z} - \phi_2^{x,z}$. Note that, due to the two-photon interference effect, finding the two photons in different spatial modes and the same temporal mode is impossible. We are thus left with the case of having two photons in the same output port (the same spatial mode), which occurs with probability $C = [p^{x,z}(0,0) + p^{x,z}(1,1) + 0.5(p^{x,z}(0,1) + p^{x,z}(1,0)) + \sqrt{p^{x,z}(0,1)p^{x,z}(1,0)}\cos(\Delta\phi^{x,z})]/b^{x,z}_{norm}$, and the case of having the photons in different temporal and spatial modes, which occurs with probability $D = [0.5(p^{x,z}(0,1) + p^{x,z}(1,0)) - \sqrt{p^{x,z}(0,1)p^{x,z}(1,0)}\cos(\Delta\phi^{x,z})]/b^{x,z}_{norm}$. This leads to

$$\begin{aligned} &P(|\psi^-\rangle|2 \text{ photons, interfering, in}) = \\ &\quad C \times P(|\psi^-\rangle|2 \text{ photons, 1 spatial mode, out}) + \\ &\quad D \times P(|\psi^-\rangle|2 \text{ photons, 2 spatial modes, 2 temporal modes, out}). \end{aligned} \tag{10}$$

4.2.3. Aggregate probability for projections onto $|\psi^-\rangle$ Now that we have calculated the conditional probabilities of a detection pattern indicating $|\psi^-\rangle$ for various inputs to the beam splitter, let us consider with what probability each case occurs. This requires that we know the photon number distribution of the pulses arriving at Charlie's beam splitter from Alice and Bob, which can be computed based on the photon number distribution at the sources and the properties of the quantum channels. For the following discussion, we assume that the channels from Alice to Charlie and from Bob to Charlie are characterized by the loss t_A and t_B, respectively, yielding pulses with number distribution $\mathbb{D}$ and mean

photon number, μt_A and σt_B, respectively. This is equivalent to assuming that no PNS attack takes place, which is the case of interest when optimizing the secret key rate in section 7[+]. We limit our discussion to the cases with two or less photons at the input of the beam splitter (but recall that the actual calculation includes up to three photons). Hence, the cases we consider and their probabilities of occurrence, P_O, are given by:

- 0 photons at the input from both sources: $P_O = \mathbb{D}_0(\mu t_A)\mathbb{D}_0(\sigma t_B)$
- 1 photon at the input from Alice and 0 from Bob: $P_O = \mathbb{D}_1(\mu t_A)\mathbb{D}_0(\sigma t_B)$
- 0 photons at the input from Alice and 1 from Bob: $P_O = \mathbb{D}_0(\mu t_A)\mathbb{D}_1(\sigma t_B)$
- 2 photons at the input from Alice and 0 from Bob: $P_O = \mathbb{D}_2(\mu t_A)\mathbb{D}_0(\sigma t_B)$
- 0 photons at the input from Alice and 2 from Bob: $P_O = \mathbb{D}_0(\mu t_A)\mathbb{D}_2(\sigma t_B)$
- 1 photon at the input from both sources: $P_O = \mathbb{D}_1(\mu t_A)\mathbb{D}_1(\sigma t_B)$

where we denote the probability of having i photons from a distribution $\mathbb{D}$ with mean number μ as $\mathbb{D}_i(\mu)$. For each of these cases, we have already computed the probability that Charlie obtains the detection pattern associated with the $|\psi^-\rangle$-state for arbitrary input states of the photons (as defined in Eq. 2). When zero or one photons arrive at the beam splitter, Eq. 3 and Eq. 4 are used, respectively. In the case in which two photons arrive from the same source, Eq. 9 is used. Finally, in the case in which one photon arrives from each source, Eq. 10 would be used in the ideal case. However, perfect indistinguishability of the photons cannot be guaranteed in practice. We characterize the degree of indistinguishability by the visibility, V, that we would observe in a closely-related Hong-Ou-Mandel (HOM) interference experiment [27] with single-photon inputs. Taking into account partial distinguishability, the probability of finding a detection pattern corresponding to the projection onto $|\psi^-\rangle$ is given by

$$\begin{aligned} &P(|\psi^-\rangle|2 \text{ photons, visibility } V, \text{ in}) = \\ &\quad VP(|\psi^-\rangle|2 \text{ photons, interfering, in}) \\ &\quad +(1-V)P(|\psi^-\rangle|2 \text{ photons, non-interfering, in}). \end{aligned} \tag{11}$$

Equations 3-11 detail all possible causes for observing the detection pattern associated with a projection onto the $|\psi^-\rangle$ Bell state, if up to two photons at the beam splitter input are taken into account. We remind the reader that all calculations in the following sections take up to three photons into account. To calculate the gains, $Q_{\mu\sigma}^{x,z}$, using these equations, we need only substitute in the correct values of μ, σ, t_A, t_B, $m^{x,z}$, $b^{x,z}$, and $\Delta\phi^{x,z}$ for the cases in which Alice and Bob both sent attenuated light pulses in the x-basis or z-basis, respectively. The error rates, $e_\mu^{x,z}$, can then be computed by separating the projections onto $|\psi^-\rangle$ into those where Alice and Bob sent photons in different states (yielding correct key bits) and in the same state (yielding erroneous key bits). More

[+] Obviously, with PNS attack (or any other eavesdropping attack that increases the error rate), the final key rate would be smaller than the one calculated under optimum conditions. However, it would still be secure.

precisely, the error rates, $e^{x,z}_{\mu\sigma}$, are calculated as $e^{x,z}_{\mu\sigma} = p^{x,z}_{wrong}/(p^{x,z}_{correct} + p^{x,z}_{wrong})$ where $p^{x,z}_{wrong}$ ($p^{x,z}_{correct}$) denotes the probability for detections yielding an erroneous (correct) bit in the x (or z)-key.

5. Characterizing experimental imperfections

The parameters used to model our system are derived from data established through independent measurements. To verify our model, the characterization of experimental imperfections in our MDI-QKD implementation [9] is very technical at times. It can be broken down into time-resolved energy measurements at the single photon level (required to extract μ, σ, $b^{x,z}$ and $m^{x,z}$ for Alice and Bob, as well as dark count and afterpulsing probabilities), measurements of phase (required to establish $\phi^{x,z}$ for Alice and Bob), and visibility measurements. In the following paragraphs we describe the procedures we followed to obtain these parameters from our system.

5.1. Our MDI-QKD Implementation

In our implementation of MDI-QKD [9] Alice's and Bob's setups are identical. Each setup consists of a CW laser emitting at 1550nm wavelength. Time-bin qubits, encoded into single photon-level light pulses with Poissonian photon number statistics, are created through an attenuator, an intensity modulator and a phase modulator located in a temperature controlled box. The two temporal modes defining each time-bin qubit are of 500 ps (FWHM) duration and are separated by 1.4 ns. Each source generates qubits at 2 MHz rate.

The time-bin qubits are sent to Charlie through an optical fiber link. The link consisted of spooled fiber (for the measurements in which Alice, Bob and Charlie were all located in the same laboratory) or deployed fiber (for the measurements in which the three parties were located in different locations within the city of Calgary). Charlie performs a BSM on the qubits he receives using a 50/50 beamsplitter and two SPDs. See Figure 4.1.2. Note that, in order to perform a Bell state measurement the photons arriving to Charlie must be indistinguishable in all degrees of freedom: polarization, frequency, time and spatial mode. The indistinguishability of the photons is assessed through a Hong-Ou-Mandel interference measurement [27]. As our system employs attenuated laser pulses, the maximum visibility we can obtain in this measurement is $V_{max} = 50\%$ (and not 100% as it would be with single photons). In our implementation the visibility measurements resulted in $V = (47 \pm 1)$, irrespective of whether they were taken with spooled fiber inside the lab, or over deployed fiber.

5.1.1. Time-resolved energy measurements First, we characterize the dark count probability per time-bin, P_d, of the SPDs (InGaAs-avalanche photodiodes operated in gated Geiger mode [26]) by observing their count rates when the optical inputs are disconnected. We then send attenuated laser pulses so that they arrive just after

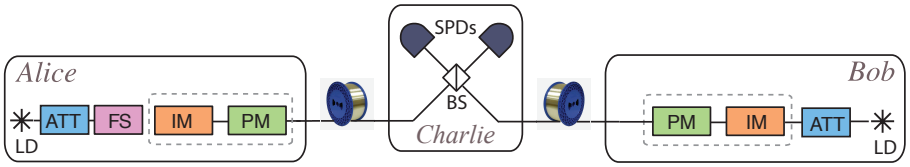


Figure 4.1.2. Time-bin qubits are created at Alice's and Bob's through a CW laser (LD), and attenuator (ATT) and temperature-controlled intensity (IM) and phase (PM) modulator. The projective measurements are done at Charlie's via a beam splitter (BS) and two single photon detectors (SPDs).

the end of the 10 ns long gate that temporarily enables single photon detection. The observed change in the count rate is due to background light transmitted by the intensity modulators (whose extinction ratios are limited) and allows us to establish $b^{x,z}$ (per time-bin) for Alice and Bob. Next, we characterize the afterpulsing probability per time-bin, P_a, by placing the pulses within the gate, and observing the change in count rate in the region of the gate prior to the arrival of the pulse. The afterpulsing model we use to assess P_a from these measurements is described below.

Once the background light and the sources of detector noise are characterized, the values of $m^{x,z}$ can be calculated by generating all required states and observing the count rates in the two time-bins corresponding to detecting photons generated in early and late temporal modes. Observe that $m^{z=1}$ for photons generated in state $|1\rangle$ (the late temporal mode) is zero (i.e. the entire optical pulse is located in the second temporal mode), since all counts in the early time-bin are attributed to one of the three sources of background described above. Furthermore, we observed that $m^{z=0}$ for photons generated in the $|0\rangle$ state (the early temporal mode) is smaller than one due to electrical ringing in the signals driving the intensity modulators. Note that, in our implementation, the duration of a temporal mode exceeds the width of a time-bin, i.e. it is possible to detect photons outside a time-bin (see Figure 4.1.3 for a schematical representation). Hence, it will be useful to also define the probability for detecting a photon arriving at any time during a detector gate; we will refer to this quantity as η_{gate}.The count rate per gate, after having subtracted the rates due to background and detector noise, together with the detection efficiency, η_{gate} (η_{gate}, as well as η, have been characterized previously based on the usual procedure [26]), allows calculating the mean number of photons per pulse from Alice or Bob (μ or σ, respectively). The efficiency coefficient relevant for our model, η, is smaller than η_{gate}. Finally, we point out that the entire characterization described above was repeated for all experimental configurations investigated to confirm the validity of the model (the configurations are detailed in Table 4.1.2). We found all parameters to be constant in $\mu\sigma t_A t_B$, with the obvious exception of the afterpulsing probability.

5.1.2. Phase measurements To detail the assessment of the phase values $\phi^{x,z}$ determining the superposition of photons in early and late temporal modes, let us

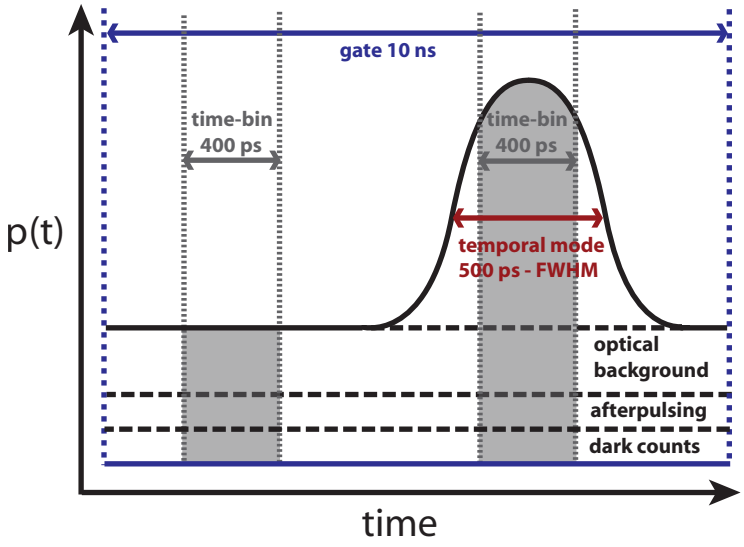


Figure 4.1.3. Sketch (not to scale) of the probability density p(t) for a detection event to occur as a function of time within one gate. Detection events can arise from a photon within an optical pulse (depicted here as a pulse in the late temporal mode), or be due to optical background, a dark count, or afterpulsing. Also shown are the 400 ps wide time-bins. Within the early time-bin only optical background, dark counts and afterpulsing give rise to detection events in this case. Note that the width of the temporal mode exceeds the widths of the time-bins.

assume for the moment that the lasers at Alice's and Bob's emit light at the same frequency. First, we defined the phase of Bob's $|+\rangle$ state to be zero (this can always be done by appropriately defining the time difference between the two temporal modes $|0\rangle$ and $|1\rangle$). Next, to measure the phase describing any other state (generated by either Alice or Bob) with respect to Bob's $|+\rangle$ state, we sequentially send unattenuated laser pulses encoding the two states through a common reference interferometer. Comparing the output intensities, we can calculate the phase difference. We note that any frequency difference between Alice's and Bob's lasers results in an additional phase difference. Its upper bound for our maximum frequency difference of 10 MHz is denoted by ϕ_{freq}.

5.1.3. Measurements of afterpulsing We now turn to the characterization of afterpulsing. After a detector click (or detection event, which includes photon detection, dark counts and afterpulsing), the probability of an afterpulse occuring due to that detection event decays exponentially with time. The SPDs are gated, with the afterpulse probability per gate being a discrete sampling of the exponential decay. This can be expressed using a geometric distribution: supposing a detection event occurred at gate $k = -1$, the probability of an afterpulse occuring in gate k is given by $P_k = \alpha p(1-p)^k$. Thus, if there are no other sources of detection events, the probability of an afterpulse occuring due to a detection event is given by $\sum_{k=0}^{\infty} \alpha p(1-p)^k$.

In a realistic situation, the geometric distribution for the afterpulses will be cut off

by other detection events, either stemming from photons, or dark counts. In addition, the SPDs have a deadtime after each detection event during which the detector is not gated until $k \geq k_{dead}$ (note that time and the number of gates applied to the detector are proportional). The deadtime can simply be accounted for by starting the above summation at $k = k_{dead}$ rather than $k = 0$. However, for an afterpulse to occur during the k^{th} gate following a particular detection event, no other detection events must have occured in prior gates. This leads to the following equation for the probability of an afterpulse per detection event:

$$P(\text{a,det}) = \sum_{k=k_{dead}}^{\infty} (\gamma \times \upsilon \times \rho \times P_k) \tag{12}$$

where:

$$\gamma = (1 - \mu_{\text{avg}}(\mu, \sigma, t_A, t_B)\eta_{gate})^{k-k_{dead}}$$

$$\upsilon = (1 - P_{d,gate})^{k-k_{dead}}$$

$$\rho = \prod_{j=k_{dead}}^{k-1} 1 - \alpha p(1-p)^j$$

$$P_k = \alpha p(1-p)^k \tag{13}$$

and $P_{d,gate}$ denotes the detector dark count probability per gate (as opposed to per time-bin), and $\mu_{\text{avg}}(\mu, \sigma, t_A, t_B)$ expresses the average number of photons present on the

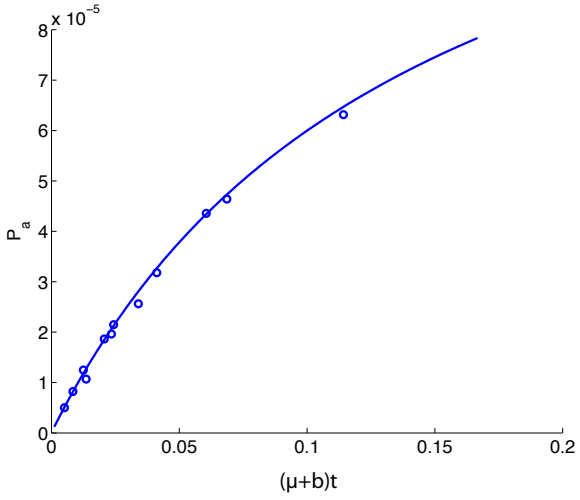


Figure 4.1.4. Afterpulse probability per time-bin as a function of the average number of photons arriving at the detector per gate.

detector during each gate as follows:

$$\mu_{\text{avg}}(\mu, \sigma, t_A, t_B) = \frac{(\mu + b_A)t_A + (\sigma + b_B)t_B}{2}, \tag{14}$$

where b_A and b_B characterize the amount of background light per gate from Alice and Bob, respectively, and the factor of $\frac{1}{2}$ comes from Charlie's beam splitter. The terms in the sum of Eq. 12 describe the probabilities of neither having an optical detection (γ), either caused by a modulated pulse or background light, nor a detector dark count (υ) in any gate before and including gate k, and not having an afterpulse in any gate before gate k (ρ), followed by an afterpulse in gate k (P_k). Equation 12 takes into account that afterpulsing within each time-bin is influenced by all detections within each detector gate, and not only those happening within the time-bins that we post-select when acquiring experimental data.

The afterpulse probability, $P_{a,gate}$, for given μ, σ, t_A and t_B can then be found by multiplying Eq. 12 by the total count rate

$$P_{a,gate} = (\mu_{\text{avg}}(\mu, \sigma, t_A, t_B)\eta_{gate} + P_{d,gate} + P_{a,gate})\, P(\text{a,det}). \tag{15}$$

This equation expresses that afterpulsing can arise from prior afterpulsing, which explains the appearance of $P_{a,gate}$ on both sides of the equation. Equation 15 simplifies to

$$P_{a,gate} = \frac{(\mu_{\text{avg}}(\mu, \sigma, t_A, t_B)\eta_{gate} + P_{d,gate})\, P(\text{a,det})}{1 - P(\text{a,det})}. \tag{16}$$

Finally, to extract the afterpulsing probability per time-bin, $P_a(\mu, \sigma, t_A, t_B)$, we note that we found that the distribution of afterpulsing across the gate to be the same as the distribution of dark counts across the gate. Hence,

$$P_a(\mu, \sigma, t_A, t_B) = P_{a,gate}\frac{P_d}{P_{d,gate}}. \tag{17}$$

Fitting our afterpulse model to the measured afterpulse probabilities, we find $\alpha = 8.63 \times 10^{-3}$, $p = 3.00 \times 10^{-2}$, and $\frac{P_d}{P_{d,gate}} = 4.96 \times 10^{-2}$ for $k_{dead} = 20$. The fit, along with the measured values, is shown in Figure 4.1.4 as a function of the average number of photons arriving at the detector per gate $\mu_{\text{avg}}(\mu, \sigma, t_A, t_B)$.
A summary of all the values obtained through these measurements is shown in Table 4.1.1.

6. Model verification

6.1. Comparing modelled with actual performance

To verify our model, we now compare its predictions with data obtained using our MDI-QKD system (our system is characterized by the parameters listed in Table 4.1.1). Experimental data is obtained using two configurations: inside the laboratory using spooled fiber (for four different distances between Alice and Bob ranging between 42

Table 4.1.1. Experimentally established values for all parameters required to describe the generated quantum states, as defined in Eq. 2, as well as two-photon interference parameters and detector properties.

Parameter	Alice's value	Bob's value
$b^{z=0} = b^{z=1}$	$(7.12 \pm 0.98) \times 10^{-3}$	$(1.14 \pm 0.49) \times 10^{-3}$
$b^{x=-} = b^{x=+}$	$(5.45 \pm 0.37) \times 10^{-3}$	$(1.14 \pm 0.49) \times 10^{-3}$
$m^{z=0}$	0.9944 ± 0.0018	0.9967 ± 0.0008
$m^{z=1}$	0	0
$m^{x=+} = m^{x=-}$	0.4972 ± 0.011	0.5018 ± 0.0080
$\phi^{z=0} = \phi^{z=1} = \phi^{x=+}$ [rad]	0	0
$\phi^{x=-}$ [rad]	$\pi + (0.075 \pm 0.015)$	$\pi - (0.075 \pm 0.015)$
Parameter	**Value**	
$\lvert\phi_{freq}\rvert$ [rad]	< 0.088	
V	0.94 ± 0.02	
P_d	$(1.83 \pm 0.77) \times 10^{-5}$	
η_{gate}	0.2	
η	0.145	

km and 103 km) and over deployed fiber (18 km). For each of these tests three different mean photon numbers (0.1, 0.25 and 0.5) were used. All the configurations tested (as well as the specific parameters used in each test) and the results obtained are listed in Table 4.1.2. In Figure 4.1.5 we show the simulated values for the error rates ($e^{z,x}$) and gains ($Q^{z,x}$) predicted by the model as a function of $\mu\sigma t_A t_B$. The plot includes uncertainties from the measured parameters, leading to a range of values (bands) as opposed to single values. The figure also shows the experimental values of $e^{z,x}$ and $Q^{z,x}$ from our MDI-QKD system in both the laboratory environment and over deployed fiber. The modelled values and the experimental results agree within experimental uncertainties over at least three orders of magnitude, from which we conclude that the model is valid for predicting error rates and gains. This now allows us to optimize performance of our QKD systems in terms of secret key rate. For instance, the model allows optimizing the mean photon number per pulse that Alice and Bob use to encode signal and decoy states as a function of transmission loss, or to identify rate-limiting components.

7. Optimization of system performance

7.1. Decoy-state analysis

To calculate secret key rates for various system parameters, which allows finding optimum conditions, first, it is necessary to compute the gain, Q_{11}^z, and the error rate, e_{11}^x, that stem from events in which both sources emit a single photon. We consider

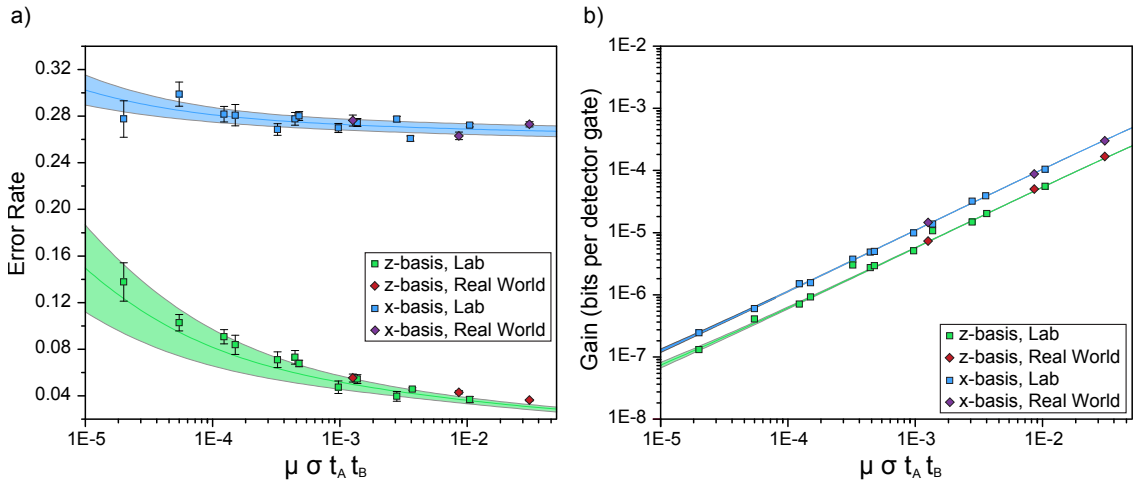


Figure 4.1.5. Modelled and measured results. Figure a) shows the plot for the error rates in the z-basis (green band) and in the x-basis (blue band) as a function of the mean photon number per pulse sent by Alice (μ) and Bob (σ) multiplied by the channel transmissions (t_A and t_B). Figure b) shows the plot of the gains as a function of $\mu\sigma t_A t_B$. The z-basis is shown in green and the x-basis is shown in blue. For both figures the results of the measurements done in the laboratory are shown with squares (blue or green) and the measurements done over deployed fiber are shown with diamond circles (red and purple). The difference in gains and error rates in the x- and the z-basis, respectively is due to the fact that, in the case in which one party sends a laser pulse containing more than one photon and the other party sends zero photons, projections onto the $|\psi^-\rangle$ Bell state can only occur if both pulses encode qubits belonging to the x-basis. The Bell state projection cannot occur if both prepare qubits belonging to the z-basis (we ignore detector noise for the sake of this argument). This causes increased gain for the x-basis and, due to an error rate of 50% associated with these projections, also an increased error rate for the x-basis.

the three-intensity decoy state method for the MDI-QKD protocol proposed in [25]*, which derives a lower bound for the secret key rate using lower bounds for $Q_{11}^{x,z}$ and an upper bound for e_{11}^{x}. Note that we assume here that imperfectly generated qubit states only affect the secret key rate through an increase of error rates. We will discuss this assumption below.

We denote the signal, decoy, and vacuum intensities by μ_s, μ_d, and μ_v, respectively, for Alice, and, similarly, as σ_s, σ_d, and σ_v for Bob♯. For the purpose of this analysis, we take both channels to have the same transmission coefficients (that is $t_A = t_B \equiv t$), according to our experimental configuration, and Alice and Bob hence both select the same mean photon numbers for each of the three intensities (that is $\mu_s = \sigma_s \equiv \tau_s$, $\mu_d = \sigma_d \equiv \tau_d$, and $\mu_v = \sigma_v \equiv \tau_v$). Additionally, for compactness of notation, we omit the μ and σ when describing the gains and error rates (e.g. we write Q_{ss}^{z} to denote the gain in the z-basis when Alice and Bob both send photons using the signal intensity).

* Note that we have corrected a mistake present in Eq. 17 of [25].
♯ Note that $\mu_v = \sigma_v = 0$ by definition.

Table 4.1.2. Measured error rates, $e^{x,z}_{\mu\sigma}$, and gains, $Q^{x,z}_{\mu\sigma}$, for different mean photon numbers, μ and σ (where $\mu = \sigma$), lengths of fiber connecting Alice and Charlie, and Charlie and Bob, ℓ_A and ℓ_B, respectively, and total transmission loss, l. The last set of data details real-world measurements using deployed fiber. Uncertainties are calculated using Poissonian detection statistics.

Fiber	$\mu = \sigma$	ℓ_A [km]	ℓ_B [km]	total loss l [dB]	$Q^x_{\mu\sigma}$	$Q^z_{\mu\sigma}$	$e^x_{\mu\sigma}$	$e^z_{\mu\sigma}$
	0.49(2)				$1.045(4) \times 10^{-4}$	$5.57(8) \times 10^{-5}$	0.272(2)	0.037(3)
Spool	0.254(9)	30.98	11.75	13.6	$3.20(2) \times 10^{-5}$	$1.47(3) \times 10^{-5}$	0.277(2)	0.040(4)
	0.101(4)				$4.84(6) \times 10^{-6}$	$2.72(6) \times 10^{-6}$	0.278(5)	0.073(6)
	0.49(2)				$3.92(2) \times 10^{-5}$	$2.02(1) \times 10^{-5}$	0.261(2)	0.046(1)
Spool	0.25(1)	40.80	40.77	18.2	$9.87(9) \times 10^{-6}$	$5.1(1) \times 10^{-6}$	0.270(4)	0.047(5)
	0.099(4)				$1.57(3) \times 10^{-6}$	$9.2(3) \times 10^{-7}$	0.281(9)	0.084(8)
	0.50(2)				$1.37(1) \times 10^{-5}$	$1.07(2) \times 10^{-5}$	0.275(3)	0.054(4)
Spool	0.24(1)	51.43	32.19	22.7	$3.73(4) \times 10^{-6}$	$3.01(8) \times 10^{-6}$	0.269(5)	0.071(7)
	0.100(6)				$6.0(1) \times 10^{-7}$	$4.07(9) \times 10^{-7}$	0.30(1)	0.103(7)
	0.50(5)				$4.96(4) \times 10^{-6}$	$2.94(3) \times 10^{-6}$	0.280(4)	0.068(3)
Spool	0.25(1)	61.15	42.80	27.2	$1.50(2) \times 10^{-6}$	$7.1(2) \times 10^{-7}$	0.282(7)	0.091(6)
	0.103(5)				$2.45(9) \times 10^{-7}$	$1.31(6) \times 10^{-7}$	0.28(2)	0.14(2)
	0.50(2)				$3.01(1) \times 10^{-4}$	$1.667(8) \times 10^{-4}$	0.273(2)	0.0362(7)
Deployed	0.26(1)	12.4	6.2	9.0	$8.78(6) \times 10^{-5}$	$5.01(4) \times 10^{-5}$	0.263(3)	0.043(1)
	0.100(4)				$1.45(2) \times 10^{-5}$	$7.3(1) \times 10^{-7}$	0.276(5)	0.055(3)

Under these assumptions, the lower bound on $Q^{x,z}_{11}$ is given by

$$Q^{x,z}_{11} \geq \frac{\mathbb{D}_1(\tau_s)\mathbb{D}_2(\tau_s)(Q^{x,z}_{dd} - Q^{x,z}_0(\tau_d)) - \mathbb{D}_1(\tau_d)\mathbb{D}_2(\tau_d)(Q^{x,z}_{ss} - Q^{x,z}_0(\tau_s))}{\mathbb{D}_1(\tau_s)\mathbb{D}_1(\tau_d)(\mathbb{D}_1(\tau_d)\mathbb{D}_2(\tau_s) - \mathbb{D}_1(\tau_s)\mathbb{D}_2(\tau_d))}, \quad (18)$$

where the various $\mathbb{D}_i(\tau)$ denote the probability that a pulse with photon number distribution $\mathbb{D}$ and mean τ contains exactly i photons, and $Q^{x,z}_0(\tau_d)$ and $Q^{x,z}_0(\tau_s)$ are given by

$$Q^{x,z}_0(\tau_d) = \mathbb{D}_0(\tau_d)Q^{x,z}_{vd} + \mathbb{D}_0(\tau_d)Q^{x,z}_{dv} - \mathbb{D}_0(\tau_d)^2 Q^{x,z}_{vv}, \quad (19)$$

$$Q^{x,z}_0(\tau_s) = \mathbb{D}_0(\tau_s)Q^{x,z}_{vs} + \mathbb{D}_0(\tau_s)Q^{x,z}_{sv} - \mathbb{D}_0(\tau_s)^2 Q^{x,z}_{vv}. \quad (20)$$

The error rate e^x_{11} can then be computed as

$$e^x_{11} \leq \frac{e^x_{dd}Q^x_{dd} - \mathbb{D}_0(\tau_d)e^x_{vd}Q^x_{vd} - \mathbb{D}_0(\tau_d)e^x_{dv}Q^x_{dv} + \mathbb{D}_0(\tau_d)^2 e^x_{vv}Q^x_{vv}}{\mathbb{D}_1(\tau_d)^2 Q^x_{11}}, \quad (21)$$

where the upper bound holds if a lower bound is used for Q^x_{11}. Note that $Q^{x,z}_{11}$, $Q^{x,z}_0(\tau_d)$, $Q^{x,z}_0(\tau_s)$ and e^x_{11} (Eqs. 18-21) are uniquely determined through measurable gains and error rates.

7.2. Optimization of signal and decoy intensities

For each set of experimental parameters (i.e. distribution function $\mathbb{D}$, channel transmissions and all parameters describing imperfect state preparation and measurement), the secret key rate (Eq. 1) can be maximized by properly selecting the intensities of the signal and decoy states (τ_s and τ_d, respectively). Here we consider its optimization as a function of the total transmission (or distance) between Alice and Bob. We make the assumptions that both the channel between Alice and Charlie and the channel between Bob and Charlie have the same transmission coefficient, t, and that Alice and Bob use phase randomized attenuated laser pulses with Poissonian photon number distribution as well as the same signal and decoy intensities. We considered values of τ_d in the range $0.01 \leq \tau_d < 0.99$ and values of τ_s in the range $\tau_d < \tau_s \leq 1$. An exhaustive search computing the secret key rate for an error correction efficiency $f = 1.14$ [28] is performed from 2 km to 200 km total distance (assuming 0.2 dB/km loss), with increments of 0.01 photons per pulse for both τ_s and τ_d. For each point, the model described in section 4 is used to compute all the experimentally accessible quantities required to compute secret key rates using the three-intensity decoy state method summarized in Eqs. 18-21.

In our optimization, we found that, in all cases, $\tau_d = 0.01$ is the optimal decoy intensity. We attribute this to the fact that τ_d has a large impact on the tightness of the upper bound on e_{11}^x in Eq. 21 (this is due to the fact that all errors in the cases in which both parties sent at least one photon, which increases with τ_d, are attributed to the case in which both parties sent exactly one photon). Figure 4.1.6 shows, as a function of total loss (or distance), the optimum values of the signal state intensity, τ_s, and the corresponding secret key rate, S, for decoy intensities of $\tau_d \in [0.01, 0.05, 0.1]$, as well as for a perfect decoy state protocol (i.e. using values of Q_{11}^z and e_{11}^x computed from the model, as detailed in the preceeding section).

7.3. Rate-limiting components

Finally, we use our model to simulate the performance of the MDI-QKD protocol given improved components. We consider two straightforward modifications to the system: replacing the InGaAs single photon detectors (SPDs) with superconducting single photon detectors (SSPDs) [29], and improving the intensity modulation (IM) system. For various combinations of these improvements, the optimized signal intensities and secret key rates for $\mu_d = 0.05$ are shown in Figure 4.1.7. First, using the state-of-the-art SSPDs in [29], the detection efficiency (η) is improved from 14.5% to 93%, and the dark count probability (P_d) is reduced by nearly two orders of magnitude. Furthermore, the mechanisms leading to afterpulsing in InGaAs SPDs are not present in SSPDs (that is $P_a = 0$). This improvement results in a drastic increase in the secret key rate and maximum distance as both the probability of projection onto $|\psi^-\rangle$ and the signal-to-noise-ratio are improved significantly. Second, imperfections in the intensity modulation system used to create pulses in our implementation contribute

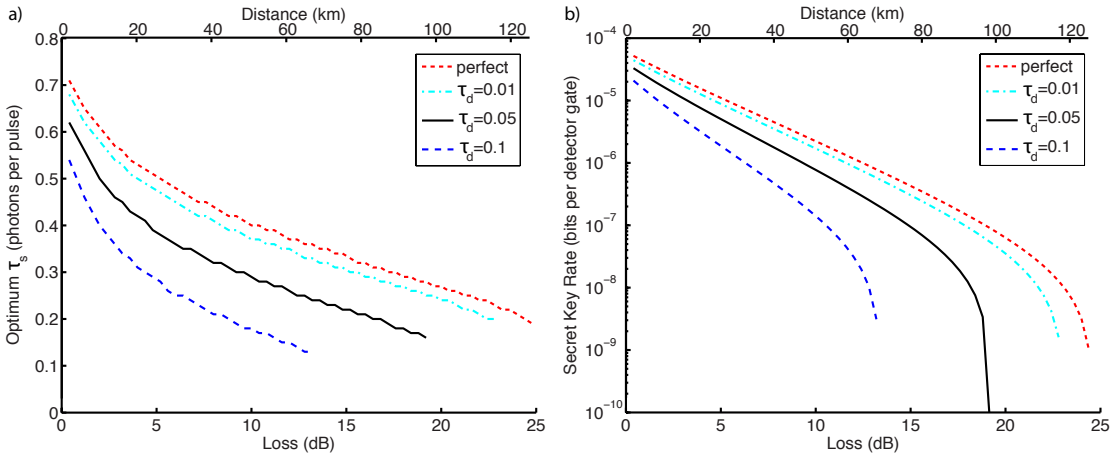


Figure 4.1.6. a) Optimum signal state intensity, τ_s, and b) corresponding secret key rate as a function of total loss in dB. The secondary axis shows distances assuming typical loss of 0.2 dB/km in optical fiber without splices. The optimum values for μ_s for small loss have to be taken with caution as in this regime the model needs to be expanded to higher photon number terms.

significantly to the observed error rates, particularly in the z-basis. Using commercially-available, state-of-the-art intensity modulators allow suppressing the DC background light (represented by $b^{x,z}$ in general quantum state given in Eq. 2) by an additional 10-20 dB, corresponding to an extinction ration of 40 dB. Furthermore, we consider improvements to the driving electronics for the intensity modulator that reduces ringing in our pulse generation by a factor of 5, bringing the values of $m^{x,z}$ in Eq. 2 closer to the ideal values. As seen in Figure 4.1.7, this provides a modest improvement to the secret key rate, both when applied to our existing implementation, and when applied in conjunction with the SSPDs.

8. Conclusion

We have developed a general model for systems implementing the Measurement-Device-Independent QKD Protocol. Our model takes into account experimental imperfections in sources and measurement devices as well as transmission loss, and is evaluated against data taken with a real, time-bin qubit-based QKD system. The consistency between observed values and predicted data confirms the model. In turn, this allows optimizing mean photon numbers for signal and decoy states and finding rate-limiting components for future improvements. We believe that our model, which is straightforward to generalize to other types of qubit encoding, as well as the detailed description of the characterization of experimental imperfections will be useful to improve QKD beyond its current state of the art.

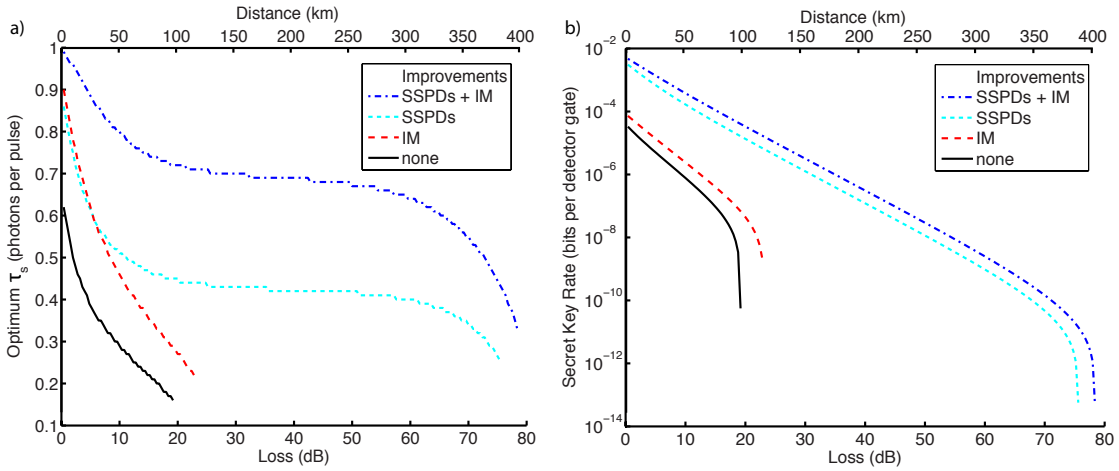


Figure 4.1.7. a) Optimum signal state intensity, τ_s, and b) corresponding secret key rate as a function of total loss in dB. The secondary axis shows distances assuming typical loss of 0.2 dB/km in optical fiber without splices. The optimum values for μ_s for small loss have to be taken with caution as in this regime the model needs to be expanded to higher photon number terms.

Acknowledgements

The authors thank E. Saglamyurek, V. Kiselyov and TeraXion for discussions and technical support, the University of Calgary's Infrastructure Services for providing access to the fiber link between the University's main campus and the Foothills campus, SAIT Polytechnic for providing laboratory space, and acknowledge funding by NSERC, QuantumWorks, General Dynamics Canada, iCORE (now part of Alberta Innovates Technology Futures), CFI, AAET and the Killam Trusts.

References

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

[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 The Security of Practical Quantum Key Disitrbution *Rev. Mod. Phys.* 81, 1301.

[3] Dixon A, Yuan Z L, Dynes J, Sharpe A W and Shields A 2010 Continuous operation of high bit rate quantum key distribution *Appl. Phys. Lett* 96, 161102.

[4] Stucki D, Walenta N, Vannel F, Thew R T, Gisin N, Zbinden H, Gray S, Towery C R and Ten S 2009 High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres *New J. Physics* 11, 075003.

[5] Schmitt-Manderbach T, Weier H, Fürst M, Ursin R, Tiefenbacher F, Scheidl T, Perdigues J, Sodnik Z, Kurtsiefer C, Rarity J. G., Zeilinger A and Weinfurter H 2007 Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km *Phys. Rev. Lett.* 98, 010504.

[6] Masanes L, Pironio S and Acín A 2011 Secure device-independent quantum key distribution with causally independent measurement devices *Nat. Comm.* 2, 238.

[7] Lo H-K, Curty M and Qi B 2012 Measurement-device-independent quantum key distribution *Phys. Rev. Lett.* 108, 130503.

[8] Braunstein S L and Pirandola S 2012 Side-channel-free quantum key distribution *Phys. Rev. Lett.* 108, 130502.
[9] Rubenok A, Slater J A, Chan P, Lucio-Martinez I, Tittel W 2013 Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks *arXiv*:1304.2463 [quant-ph].
[10] Liu Y, Chen T-Y, Wang L-J, Liang H, Shentu G-L, Wang J, Cui K, Yin H-L, Liu N-L, Li L, Ma X, Pelc, J S, Fejer M M, Zhang Q, Pan J-W 2012 Experimental measurement-device-independent quantum key distribution *arXiv*:1209.6178 [quant-ph].
[11] da Silva T F, Vitoreti D, Xavier G B, Temporão G P and von der Weid J P 2012 Proof-of-principle demonstration of measurement device independent QKD using polarization qubits *arXiv*:1207.6345 [quant-ph].
[12] Brassard G, Lütkenhaus N, Mor T, Sanders B 2000 Limitation on practical quantum cryptography *Phys. Rev. Lett.* 85, 1330.
[13] Hwang W 2003 Quantum Key Distribution with High Loss: Towards Global Secure Communication *Phys. Rev. Lett.* 91, 057901.
[14] Lo H-K, Ma X and Chen K 2005 Decoy State Quantum Key Distribution *Phys. Rev. Lett.* 94, 230504.
[15] Wang X 2005 Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptoraphy *Phys. Rev. Lett.* 94, 230503.
[16] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 Trojan-horse attacks on quantum-key-distribution systems *Phys. Rev.* A 73, 022320.
[17] Fung C-H F, Qi B, Tamaki K and Lo H-K 2007 Phase-remapping attack in practical quantum key distribution systems *Phys. Rev. A* 75, 032314.
[18] Lamas-Linares A and Kurtsiefer C 2007 Breaking a quantum key distribution system through a timing side channel *Opt. Express* 15, 9388.
[19] Zhao Y, Fung C-H F, Qi B, Chen C and Lo H-K 2008 Quantum Hacking: Experimental demonstration of time-shift attack against practical quantum key distribution systems *Phys. Rev. A* 78, 042333.
[20] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 Thermal blinding of gated detectors in quantum cryptography *Opt. Express* 18, 27938.
[21] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 Hacking commercial quantum cryptography systems by tailored bright illumination *Nat. Photonics* 4, 686.
[22] Yuan Z L, Dynes J F and Shields A J 2010 Avoiding the blinding attack in QKD *Nat. Phot.* 4, 800.
[23] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 Avoiding the blinding attack in QKD *Nat. Phot.* 4, 801.
[24] Bennett C and Brassard G 1984 Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, 175.
[25] Wang X-B 2013 Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors *Phys. Rev. A* 87, 012320.
[26] Stucki D, Ribordy G, Stefanov A, Zbinden H, Rarity J and Wall T 2001 Photon counting for quantum key distribution with Peltier cooled InGaAs/InP APDs *J. of Mod. Opt.* 48, 1967.
[27] Hong C K, Ou Z Y and Mandel L 1987 Measurement of subpicosecond time intervals between two photons by interference *Phys. Rev. Lett.* 59, 2044.
[28] Sasaki M *et. al.* 2011 Field test of quantum key distribution in the Tokyo QKD Network *Opt. Express* 19, 10387.
[29] Marsili F, Verma V B, Stern J A , Harrington S, Lita A E, Gerrits T, Vayshenker I, Baek B, Shaw M D, Mirin R P and Nam S W 2013 Detecting single infrared photons with 93% system efficiency *Nat. Phot.* 7, 210.

Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks

A. Rubenok,[1,2] J. A. Slater,[1,2] P. Chan,[1,3] I. Lucio-Martinez,[1,2] and W. Tittel[1,2]

[1] *Institute for Quantum Science & Technology, University of Calgary, Canada*
[2] *Department of Physics & Astronomy, University of Calgary, Canada*
[3] *Department of Electrical and Computer Engineering, University of Calgary, Canada*

Several vulnerabilities of single photon detectors have recently been exploited to compromise the security of quantum key distribution (QKD) systems. In this letter we report the first proof-of-principle implementation of a new quantum key distribution protocol that is immune to any such attack. More precisely, we demonstrated this new approach to QKD in the laboratory over more than 80 km of spooled fiber, as well as across different locations within the city of Calgary. The robustness of our fibre-based implementation, together with the enhanced level of security offered by the protocol, confirms QKD as a realistic technology for safeguarding secrets in transmission. Furthermore, our demonstration establishes the feasibility of controlled two-photon interference in a real-world environment, and thereby removes a remaining obstacle to realizing future applications of quantum communication, such as quantum repeaters and, more generally, quantum networks.

Quantum key distribution (QKD) promises the distribution of cryptographic keys whose secrecy is guaranteed by fundamental laws of quantum physics[1, 2]. Starting with its invention in 1984[3], theoretical and experimental QKD have progressed rapidly. Information theoretic security, which ensures that secret keys can be distributed even if the eavesdropper, Eve, is only bounded by the laws of quantum physics, has been proven under various assumptions about the devices of the legitimate QKD users, Alice and Bob[4, 5]. Furthermore, experimental demonstrations employing quantum states of light have meanwhile resulted in key distribution over more than 100 km distance through optical fiber[6] or air[7], QKD networks employing trusted nodes[8], as well as in commercially available products[9].

However, it became rapidly clear that some of the assumptions made in QKD proofs were difficult to meet in real implementations, which opened side channels for eavesdropping attacks. The most prominent examples are the use of quantum states encoded into attenuated laser pulses as opposed to single photons[10], and, more recently, various possibilities for an eavesdropper to remote-control or monitor single photon detectors[11–14]. Fortunately, both side channels can be removed using appropriately modified protocols. In the first case, randomly choosing between so-called signal or decoy states (quantum states encoded into attenuated laser pulses with different mean photon numbers) allows one to establish a secret key strictly from information conveyed by single photons emitted by the laser[15–17]. (We remind the reader that an attenuated laser pulse comprising on average μ photons contains exactly one photon with probability $P_1(\mu) = \mu e^{-\mu}$ [10].) Furthermore, the recently proposed measurement-device independent (MDI) QKD protocol[18] (for closely related work see [19]) additionally ensures that controlling or monitoring detectors, regardless by what means, does not help the eavesdropper to gain information about the distributed key. Note that, while the two most prominent side channels are removed by MDI-QKD, others remain open and have to be closed by means of appropriate experimental design (see the Supplemental Material).

The MDI-QKD protocol is a clever time-reversed version of QKD based on the distribution and measurement of pairs of maximally entangled photons[20]: In the idealized version, Alice and Bob randomly and independently prepare single photons in one out of the four qubit states $|\psi\rangle_{A,B} \in [|0\rangle, |1\rangle, |+\rangle, |-\rangle]$, where $|\pm\rangle = 2^{-1/2}(|0\rangle \pm |1\rangle)$. The photons are then sent to Charlie, who performs a Bell state measurement, i.e. projects the photons' joint state onto a maximally entangled Bell state[21]. Charlie then publicly announces the instances in which his measurement resulted in a projection onto $|\psi^-\rangle \equiv 2^{-1/2}\big(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\big)$ and, for these cases, Alice and Bob publicly disclose the bases (z, spanned by $|0\rangle$ and $|1\rangle$, or x, spanned by $|\pm\rangle$) used to prepare their photons. (They keep their choices of states secret.) Identifying quantum states with classical bits (e.g. $|0\rangle, |-\rangle \equiv 0$, and $|1\rangle, |+\rangle \equiv 1$) and keeping only events in which Charlie found $|\psi^-\rangle$ and they picked the same basis, Alice and Bob now establish anti-correlated key strings. (Note that a projection of two photons onto $|\psi^-\rangle$ indicates that the two photons, if prepared in the same basis, must have been in orthogonal states.) Bob then flips all his bits, thereby converting the anti-correlated strings into correlated ones. Next, the so-called *x-key* is formed out of all key bits for which Alice and Bob prepared their photons in the x-basis; its error rate is used to bound the information an eavesdropper may have acquired during photon transmission. Furthermore, Alice and Bob form the *z-key* out of those bits for which both picked the z-basis. Finally, they perform error correction and privacy amplification[1, 2] to the *z-key*, which results in the secret key.

As in the entanglement-based protocol, the time-reversed version ensures that Eve cannot gain informa-

tion by eavesdropping photons during transmission or by modifying the device that generates entanglement – either the source of photon pairs or the projective two-photon measurement, respectively – without leaving a trace[22, 23]. Furthermore, the outstanding attribute of the MDI-QKD protocol is that it de-correlates detection events (here indicating a successful projection onto the $|\psi^-\rangle$ Bell state) from the values of the x- and z-*key* bits and hence the secret key bits. In other words, all side channels related to the detection setup, regardless whether actively attacked or passively monitored, do not help Eve gain information about the secret key.

Unfortunately, the described procedure is currently difficult to implement for two reasons, first of which is the lack of practical single photon sources. However, it is possible to replace the true single photons by attenuated laser pulses of varying mean photon number (i.e. signal and decoy states, as introduced above), and to establish the secret key using information only from joint measurements at Charlie's that stem from Alice and Bob both sending single photons[24]. This procedure results in the same security against eavesdropping as the conceptually simpler one discussed above. The secret key rate, S, distilled from signal states, is then given by[18]:

$$S \geq Q_{11}^z\big(1 - h_2(e_{11}^x)\big) - Q_{\mu\sigma}^z f h_2(e_{\mu\sigma}^z), \qquad (1)$$

where $h_2(X)$ denotes the binary entropy function evaluated on X, and f describes the efficiency of error correction with respect to Shannon's noisy coding theorem. Furthermore, Q_{11}^z, e_{11}^x, $Q_{\mu\sigma}^z$, and $e_{\mu\sigma}^z$ are gains (Q – the probability of a projection onto $|\psi^-\rangle$ per emitted pair of pulses) and error rates (e – the ratio of erroneous to total projections onto $|\psi^-\rangle$) in either the x- or z-basis for Alice and Bob sending single photons (denoted by subscript "11"), or for pulses emitted by Alice and Bob with mean photon number μ and σ (denoted by subscript "$\mu\sigma$"), respectively. While the latter are directly accessible from experimental data, the former have to be calculated using a decoy state method [18, 24] (see the Supplemental Material).

Second, a crucial element for MDI-QKD as well as future quantum repeaters and networks is a Bell state measurement (BSM)[25]. However, this two-photon interference measurement has not yet been demonstrated with photons that were generated by independent sources and have travelled through separate deployed fibers (i.e. fibers that feature independent changes of propagation times and polarization transformations). To implement the BSM one requires that these photons be indistinguishable, i.e. arrive simultaneously within their respective coherence times, with equal polarization, and feature sufficient spectral overlap. Yet, due to time-varying properties of optical fibers in a real-world environment, significant changes to photons' indistinguishability can happen in less than a minute, as depicted in Fig. 4.2.1.

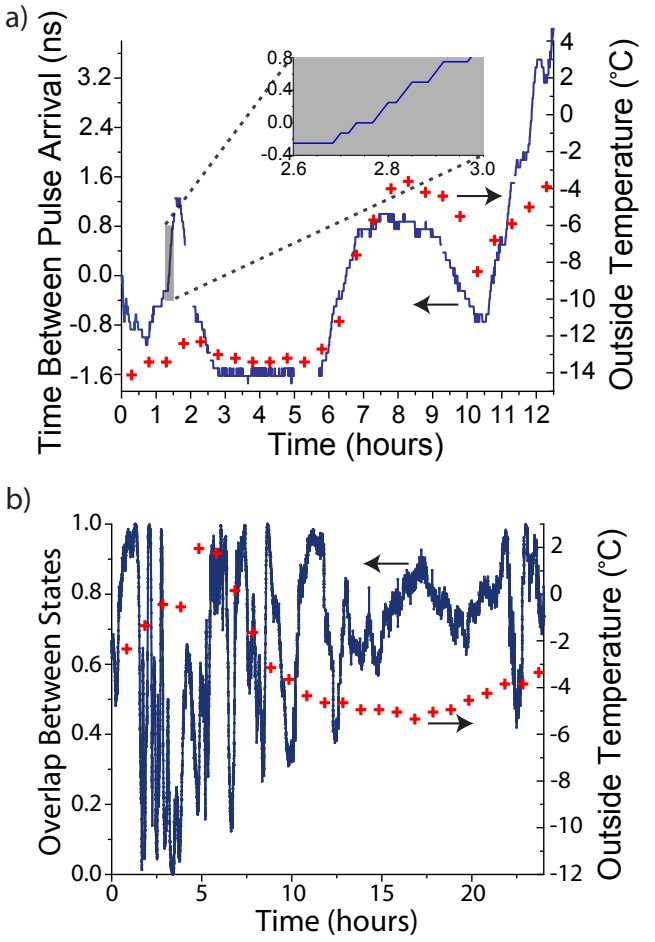


FIG. 4.2.1. (a) Drift of differential arrival time. Variation of arrival time difference of attenuated laser pulses emitted at Alice's and Bob's after propagation to Charlie. (b) Variation in the overlap of the polarization states of originally horizontally polarized light (emitted by Alice and Bob) after propagation to Charlie. Both panels include temperature data (crosses), showing correlation between variations of indistinguishability and temperature. In addition, despite local frequency locks, the difference between the frequencies of Alice's and Bob's lasers varied by up to 20 MHz per hour (not shown).

Furthermore, the carrier frequencies of the signals generated at Alice's and Bob's generally vary. These instabilities make real-world Bell state measurements without stabilization by means of active feedback impossible.

Hence, to enable MDI-QKD and pave the way for quantum repeaters and quantum networks, we developed the ability to track and stabilize photon arrival times and polarization transformations as well as the frequency difference between Alice's and Bob's lasers during all measurements (for more information see the Supplemental Material). In order to ensure the indistinguishability of

Setup	Fiber	ℓ_A [km]	l_A [dB]	ℓ_B [km]	l_B [dB]	total length ℓ [km]	total loss l [dB]
1a	Spool	22.85	4.6	22.55	4.5	45.40	9.1
1b	Spool	30.98	6.8	34.65	6.9	65.63	13.7
1c	Spool	40.80	9.1	40.77	9.1	81.57	18.2
2	Deployed	12.4	4.5	6.2	4.5	18.6	9.0

TABLE 4.2.1. Length and loss (ℓ_A, l_A, ℓ_B, l_B) of the individual fiber links used to connect Alice and Charlie, and Charlie and Bob, respectively, for all tested setups. The table also lists the total length ℓ and total loss $l = l_A + l_B$ (in dB). The last line details measurements outside the laboratory with deployed fiber.

photons arriving at Charlie's and to allow, for the first time, Bell state measurements in a real-world environment, we developed and implemented three stabilization systems (see Fig. 4.2.2): fully-automatic polarization stabilization, manual adjustment of photon arrival time, and manual adjustment of laser frequency. Note that automating the frequency and timing stabilization systems is straightforward, particularly if the active control elements are placed in Charlie's setup.

We verified that we could indeed maintain the indistinguishability of the photons by frequently measuring the visibility, V_{HOM}, of the so-called Hong-Ou-Mandel dip[26] (a two-photon interference experiment that is closely related to a BSM). On average we found V_{HOM}=47±1%, which is close to the maximum value of 50% for attenuated laser pulses with a Poissonian photon number distribution[27], and thereby confirm that real-world two-photon interference is possible.

To assess the feasibility of MDI-QKD, we implemented a proof-of-principle demonstration of MDI-QKD using the decoy state protocol proposed by Wang[24]. This protocol requires that Alice and Bob choose between three different mean photon numbers: two non-zero values referred to as signal and decoy as well as vacuum. We performed our experiments over four different distances (henceforth referred to as setups) comprising two different arrangements (see Fig. 4.2.2): (i) Alice, Bob and Charlie are located within the same lab, and Alice and Bob are connected to Charlie via separate spooled fibers of various lengths and loss. (ii) Alice, Bob and Charlie are located in different locations within the city of Calgary, and Alice and Bob are connected to Charlie by deployed fibers of 12.4 and 6.2 km length, respectively. The fiber lengths and loss in each setup are listed in Table 1.

For each setup, we prepared all 4 combinations of Alice and Bob picking a state from the z-basis (i.e. $|\psi\rangle_{A,B} \in [|0\rangle, |1\rangle]$, where $|0\rangle$ and $|1\rangle$ denote time-bin qubits[21] prepared in an early or late temporal mode), and all 4 combinations of picking a state from the x-basis (i.e. $|\psi\rangle_{A,B} \in [|+\rangle, |-\rangle]$). Using a detailed model of our MDI-QKD system[28], we calculated the signal and decoy

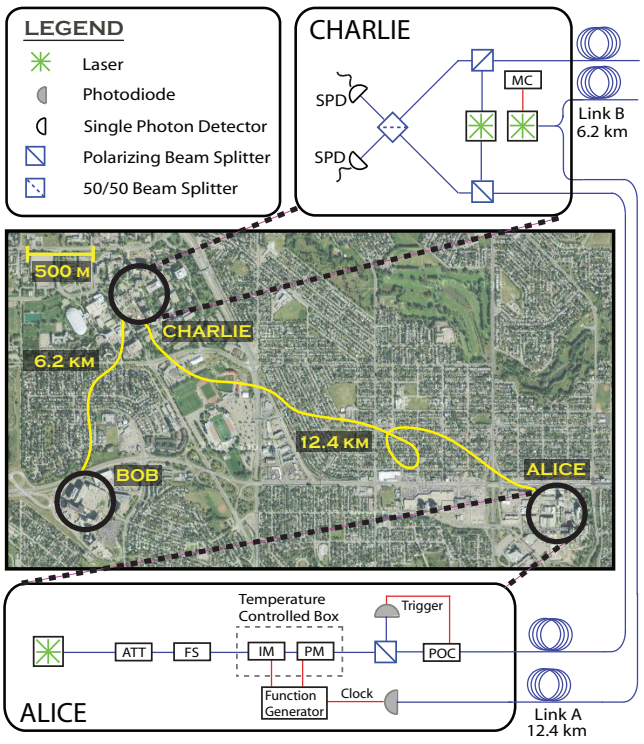


FIG. 4.2.2. Aerial view showing Alice (located at SAIT Polytechnic), Bob (located at the University of Calgary (U of C) Foothills campus) and Charlie (located at the U of C main campus). Also shown is the schematic of the experimental setup. Optically synchronized using a master clock (MC) at Charlie's, Alice and Bob (not shown; setup identical to Alice's) generated time-bin qubits at 2 MHz rate encoded into Fourier-limited attenuated laser pulses using highly stable continuous-wave lasers at 1552.910 nm wavelength, temperature-stabilized intensity and phase modulators (IM, PM), and variable attenuators (ATT). The two temporal modes defining each time-bin qubit were of 500 ps (FWHM) duration and were separated by 1.4 ns. The qubits travelled through 12.4 and 6.2 km of deployed optical fibers to Charlie, where a 50/50 beam splitter followed by two gated (10 μs deadtime) InGaAs single photon detectors (SPD) allowed projecting the bi-partite state onto the $|\psi^-\rangle$ Bell state. (This projection occurred if the two detectors indicate detections with 1.4±0.4 ns time difference.) The MC, polarization controller (POC) and Alice's frequency shifter (FS) are used to maintain indistinguishability of the photons upon arrival at Charlie. These three feedback systems are detailed in the Supplemental Material. The individual setups for measurements using spooled fiber (arrangement (i)) are identical.

intensities that maximize the secret key rate produced by the decoy-state method for each setup. For our decoy intensity we generated attenuated laser pulses containing on average $\mu = \sigma = 0.05 \pm 5\%$ photons and for our signal intensities we used a mean photon number between 0.25 and 0.5 (the optimal value depends on loss). For each of

the four distance configurations listed in Table 1, and for each of the 16 pairs of qubit states, we performed measurements of all 9 combinations of Alice and Bob using the signal, decoy or vacuum intensity. We recorded the number of joint detections in which one detector indicated an early arriving photon (or an early noise count), and the other detector indicated a late arriving photon (or a late noise count), which, for time-bin qubits, is regarded as a projection onto the $|\psi^-\rangle$-state[21]. Depending on the observed detection rates, measurements took between 2 and 35 minutes. This data yields the gains, $Q^z_{\mu\sigma}$ and $Q^x_{\mu\sigma}$, and error rates, $e^z_{\mu\sigma}$ and $e^x_{\mu\sigma}$, a subset of which is plotted in Fig. 4.2.3a. A complete list of gains and error rates is presented in the Supplemental Material.

We then computed secret key rates according to Eq. 1 after extracting Q^z_{11} and e^x_{11} using Wang's decoy state calculation[24] and assuming an error correction efficiency f=1.14[8]. As shown in Fig. 4.2.3b, all our measurements, both outside and inside the laboratory, and using up to 80 km of spooled fiber between Alice and Bob, output a positive secret key rate. Furthermore, using our model[28], we estimate that our setup allows secret key distribution up to a total loss of 18±4.8 dB, which is in agreement with our QKD results. Assuming the standard loss coefficient for telecommunication fibers without splices of 0.2 dB/km, this value corresponds to a maximum distance between Alice and Bob of 90±24 km. Note that moving from our proof-of-principle demonstration to the actual distribution of secret keys requires additional developments, which are detailed in the Supplemental Material.

In summary, we have demonstrated that real-world quantum key distribution with practical attenuated laser pulses and immunity to detector hacking attacks is possible using current technology. Our setup contains only standard, off-the-shelf components, its development into a complete QKD system follows well-known steps[8], and the extension to higher key rates using state-of-the-art detectors[29, 30] is straightforward. We also point out that MDI-QKD is well suited for key distribution over long distances, and we expect that further developments will rapidly push the separation between Alice and Bob beyond its current maximum of 250 km[6]. Finally, we remind the reader that the demonstrated possibility for Bell state measurements in a real-world environment and with truly independent photons also removes a remaining obstacle to building a quantum repeater, which promises quantum communication such as QKD over arbitrary distances.

Note added: We note that related experimental work has recently been reported in http://arxiv.org/abs/1207.0392 and http://arxiv.org/abs/1209.6178.

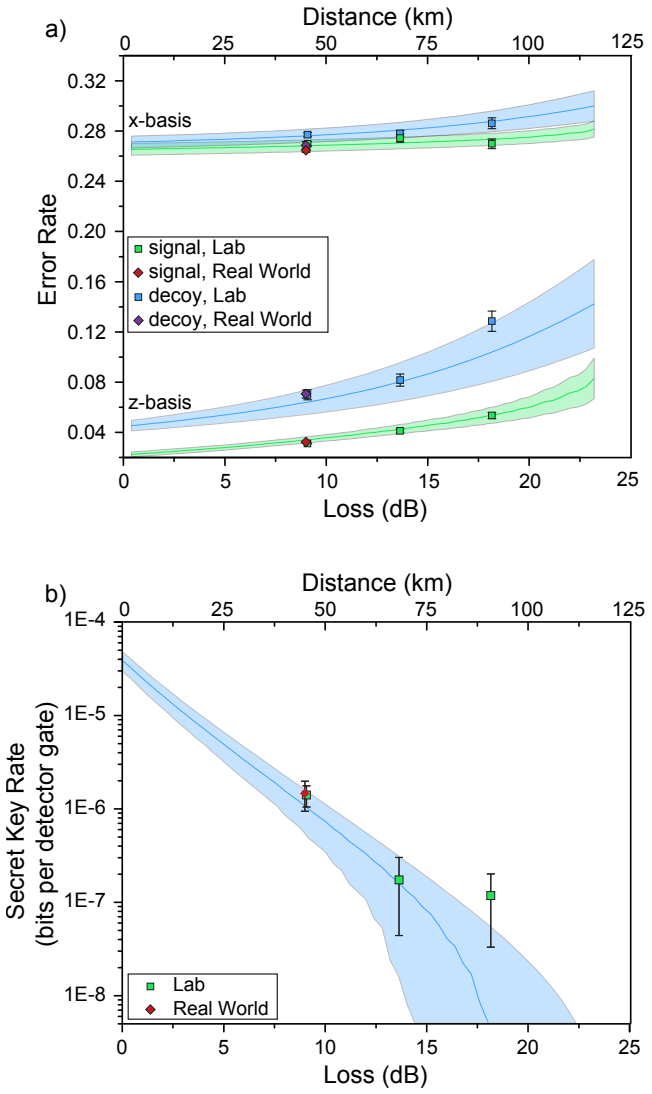


FIG. 4.2.3. (a) Measured error rates $e^z_{\mu\sigma}$ and $e^x_{\mu\sigma}$ for Alice and Bob either both using signal intensity or both using decoy intensity as a function of total loss, $l = l_A + l_B$ (in dB). We note that every other combination of intensities used in the decoy-state analysis requires Alice or Bob (or both) sending vacuum, and thus the error rate is 50% and not plotted. (b) Experimentally obtained and simulated secret key rates as a function of total loss, $l = l_A + l_B$ (in dB), with $l_A \cong l_B$, for optimized mean photon numbers. Experimental secret key rates are directly calculated from measured gains and error rates using the decoy state method[24] (see Supplemental Material for details). In both panels, the secondary x-axis shows distance assuming loss of 0.2 dB/km. Diamonds depict results obtained using deployed fibers (see Fig. 4.2.2a); all other data was obtained using fiber on spools. Uncertainties (one standard deviation) were calculated for all measured points assuming Poissonian detection statistics. We stress that the simulated values, computed using our model[28], do not stem from fits but are based on parameters that have been established through independent measurements. Monte-Carlo simulations using uncertainties in these measurements lead to predicted bands as opposed to lines (for more details see the Supplemental Material).

ACKNOWLEDGEMENTS

The authors thank E. Saglamyurek, V. Kiselyov and TeraXion for discussions and technical support, the University of Calgary's Infrastructure Services for providing access to the fiber link between the University's main campus and the Foothills campus, SAIT Polytechnic for providing laboratory space, and acknowledge funding by NSERC, QuantumWorks, General Dynamics Canada, iCORE (now part of Alberta Innovates Technology Futures), CFI, AAET and the Killam Trusts.

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

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

[3] C. H. Bennett and G. Brassard, Quantum cryptography: public key distribution and coin tossing. *Proc. Int. Conf. on Computer Systems and Signal Processing* (Bangalore, 1984) (New York: IEEE), pp. 175-179.

[4] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85,** 441-444 (2000).

[5] D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, Security of quantum key distribution with imperfect devices. *Quant. Inf. Comp.* **4,** 325-360 (2004).

[6] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery and S. Ten, High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Physics* **11,** 075003 (2009).

[7] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, Th. Scheidl, J. Perdigues, Z. Sodnik, J. G. Rarity, A. Zeilinger and H. Weinfurter, Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. *Phys. Rev. Lett.* **98,** 010504 (2007).

[8] M. Sasaki *et al.* Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **19** (11), 10387-10409 (2011).

[9] http://www.idquantique.com, http://www.magiqtech.com.

[10] G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders, Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **85,** 1330-1333 (2000).

[11] A. Lamas-Linares and C. Kurtsiefer, Breaking a quantum key distribution system through a timing side channel, *Opt. Express*, **15** (15), 9388-9393 (2007).

[12] 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,** 042333 (2008).

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

[14] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, Thermal blinding of gated detectors in quantum cryptography. *Opt. Express* **18** (26), 27938-27954 (2010).

[15] W. Hwang, Quantum key distribution with high loss: Towards global secure communication. *Phys. Rev. Lett.* **91,** 057901 (2003).

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

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

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

[19] S. L. Braunstein & S. Pirandola, Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).

[20] C. H. Bennett, G. Brassard and N. D. Mermin, Quantum cryptography without Bells theorem. *Phys. Rev. Lett.* **68,** 557-559 (1992).

[21] W. Tittel and G. Weihs, Photonic entanglement for fundamental tests and quantum communication. *Quant. Inf. Comp.* **1**(2), 3-56 (2001).

[22] E. Biham, B. Huttner and T. Mor, Quantum cryptographic network based on quantum memories. *Phys. Rev. Lett.* **54**, 2651-2658 (1996).

[23] H. Inamori, Security of Practical Time-Reversed EPR Quantum Key Distribution. *Algorithmica* **34,** 340-365 (2002).

[24] X.-B. Wang, Three-intensity decoy state method for device independent quantum key distribution with basis dependent errors. http://arxiv.org/abs/1207.0392.

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

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

[27] L. Mandel, Photon interference and correlation effects produced by independent quantum sources. *Phys. Rev. A* **28,** 929-943 (1983).

[28] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez and W. Tittel, Modelling MDI-QKD http://arxiv.org/abs/1204.0738.

[29] Z. L. Yuan, A. W. Sharpe, J. F. Dynes, A. R. Dixon and A. J. Shields, Multi-gigahertz operation of photon counting InGaAs avalanche photodiodes. *Appl. Phys. Lett.* **96,** 071101 (2010).

[30] 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. *arXiv:1209.5774* (2012).

Chapter 5

Quantum Entanglement for Quantum Repeaters

A goal of quantum communication is the distribution of entanglement between faraway locations. This long-distance entanglement could be used for long-distance fundamental tests of quantum mechanics, such as Bell inequalities, and also practical applications like quantum cryptography protocols, such as MDI-QKD. Unfortunately, as discussed earlier, exponentially-scaling loss in any communication channel limits the practical distance over which entanglement can be established. To break this distance barrier and allow for truly long-distance quantum communication one must develop a new quantum technology - the quantum repeater.

As explained in Chapter 1, a long channel can be split into a series of smaller, elementary links, which are connected via quantum repeaters. These repeaters generate entangled photons, store one photon per entangled pair in quantum memories, distribute the other half across the elementary link and then use entanglement swapping to link distant elementary links together. A long-term goal of the QC2 group is to develop a functioning quantum repeater.

The motivation for the work presented in this chapter is to demonstrate key steps towards this long term goal: interfacing sources of photonic entanglement with suitable quantum memories and testing necessary features of a quantum memory. In the repeater architecture we consider, the qubit is input to a quantum memory and, in the ideal scenario, recalled from the memory at a later time without any changes to its quantum state. Moreover, as entanglement swapping and BSMs are required for quantum repeaters, there needs to be no changes to any degree of freedom of the photons during storage and furthermore, entanglement must be preserved. One challenge in these projects was developing a source

of entanglement to interface with a quantum memory. Typical SPDC photon pair sources have bandwidths in the terahertz regime while typical quantum memories have bandwidths around tens of megahertz. Our group's Entanglement team and Memory team were able to meet half-way and develop technologies working around several gigahertz.

This chapter contains three articles. In the first we describe how we used our photon pair source to generate a conditional time-bin qubit, which was stored and recalled in the quantum memory. We demonstrated that the fidelity of the time-bin quantum state storage was higher than any classical memory could achieve. Also, the conditioning is closely related to heralded state storage, which is necessary for quantum repeaters (see Chapter 1). In the second article, we showed that there was no change to any degree of freedom during storage. To demonstrate this, we performed two-photon interference experiments with photons recalled from separate quantum memories and also BSMs with two qubits, one of which was stored in a quantum memory. The high visibility of the interference and low error rate of the BSM confirm that no degree of freedom is significantly modified during storage. Note that in these experiments, we used attenuated laser pulses instead of the photon pair source as two inputs were required. In the third article, we upgraded our photon pair source to a source of entanglement and demonstrated the faithful storage of entanglement. These works demonstrate that our quantum memories are suitable for quantum repeaters.

The fabrication of the quantum memory material was done by Prof. Wolfgang Sohler's group at the University of Paderborn and the quantum memories were designed and developed by our QC2 Memory team. In collaboration with Jeongwan Jin and Félix Bussières, I focused on the development of the optical sources for all three projects, as well as performing the measurements and analyzing the results.

Conditional detection of pure quantum states of light after storage in a Tm-doped waveguide

Erhan Saglamyurek,[1] Neil Sinclair,[1] Jeongwan Jin,[1] Joshua A. Slater,[1] Daniel Oblak,[1]
Félix Bussières,[1,*] Mathew George,[2] Raimund Ricken,[2] Wolfgang Sohler,[2] and Wolfgang Tittel[1]

[1] *Institute for Quantum Information Science, and Department of Physics & Astronomy, University of Calgary, 2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada*
[2] *Department of Physics - Applied Physics, University of Paderborn, Warburger Str. 100, 33095 Paderborn, Germany*

We demonstrate the conditional detection of time-bin qubits after storage in and retrieval from a photon-echo based waveguide quantum memory. Each qubit is encoded into one member of a photon-pair produced via spontaneous parametric down conversion, and the conditioning is achieved by the detection of the other member of the pair. Performing projection measurements with the stored and retrieved photons onto different bases we obtain an average storage fidelity of 0.885 ± 0.020, which exceeds the relevant classical bounds and shows the suitability of our integrated light-matter interface for future applications of quantum information processing.

Quantum memories are key elements for future applications of quantum information science such as long-distance quantum communication via quantum repeaters [1, 2] and, more generally, distributed quantum information processing in quantum networks [3]. They enable reversible mapping of arbitrary quantum states between travelling and stationary carriers (i.e. light and matter). This reduces the impact of loss on the time required to establish entanglement between distant locations [1], and allows the implementation of local quantum computers based on linear optics [4]. However, towards these ends, the successful transfer of a quantum state into the memory must be announced by a heralding signal. When using an individual absorber, such a signal can be derived through the detection of a change of atomic level population [5]. In atomic ensembles, this approach is infeasible. Instead, storage is derived from the detection of a second photon that either indicates the absorption [6], or the presence of the first at the input of the memory [7] (the first approach relies on spontaneous Raman scattering, the second on using pairs of photons). Furthermore, quantum memories must have large acceptance bandwidths and multi-mode capacities, and allow on-demand read-out after second-long storage with high efficiency [7, 8]. In addition, for viable quantum technology, quantum memories should be robust and simple to operate (e.g. be based on integrated optics).

A lot of progress towards these figures of merit has been reported over the past few years, including work that explores electromagnetically induced transparency (EIT), as well as photon-echo and cavity QED-based approaches (see [2, 5, 7–16] for reviews and latest achievements). For instance, quantum memories employing Rb vapour have demonstrated efficiencies up to 87% [9] and storage times in excess of 0.1 s [10], while GHz bandwidths [11] and storage of 64 modes [14] have been shown in rare-earth materials. However, having a quantum memory that simultaneously satisfies all figures of merit currently remains an outstanding challenge.

Yet, strictly, most of these experiments did not report true heralding – either heralding was not actually implemented, or the 'heralding' signal was generated only after the stored photon left the memory, or the signal could, due to technical issues, only be derived once the stored photon was detected. Nevertheless, experiments that employ photon pairs [11–13, 17] do gain from conditioning the detection of the stored photon on that of the auxiliary photon (i.e. *a posteriori* 'heralding'): by reducing the effects of loss and detector noise conditioning generally increases the fidelity between the quantum state of the original and the retrieved photon.

Supplementing the experiments on storage of entangled photons [11–13, 17], we now report another step towards the goal of building universal, viable, and heralded quantum memory devices – the storage of photons in pure quantum states in a solid state waveguide, their retrieval, and their conditional detection by means of temporal correlations with auxiliary photons. We point out that the step to true heralding is minor and of purely technical nature; it simply requires using different, existing, single-photon detectors (see, e.g., [18, 19]).

Our experimental setup consists of two main blocks, see Fig. 5.1.1: A spontaneous parametric down-conversion (SPDC) photon-pair source, and a Ti:Tm:$LiNbO_3$ single mode waveguide fabricated by in-diffusion processes [20]. When cooled to 3 K, and using a photon-echo quantum memory protocol [7, 8, 21], the Tm-doped waveguide allows storage and retrieval of quantum states encoded into one member of each photon pair, while the detection of the other member provides the conditioning signal.

In the photon-pair source a mode-locked pump laser generates 6 ps long pulses at a rate of 80 MHz and 1047.328 nm central wavelength. They are subsequently frequency-doubled (FD) in a periodically poled $LiNbO_3$ (PPLN) crystal, yielding pulses with 523.664 nm cen-

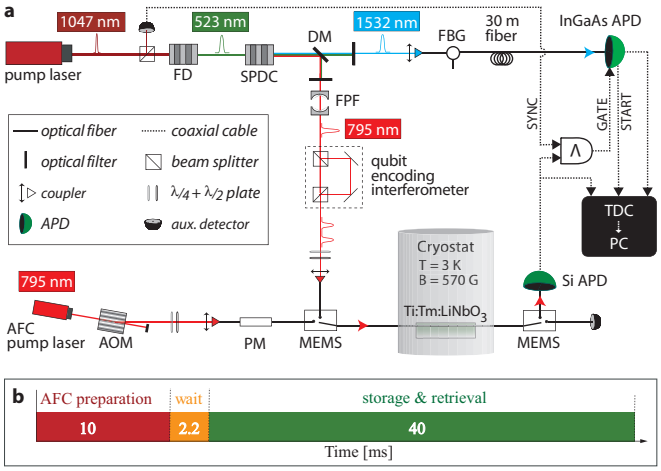


FIG. 5.1.1. **a.** Photon pair source and quantum memory setup (see text for details). Wave-plates align light polarization along the $LiNbO_3$'s C_3-axis. The waveguide is held at 3 K, and a 570 G magnetic field is applied along the crystal's C_3-axis (see Fig. 2a). **b.** Timing sequence containing three repeated phases: 10 ms *AFC preparation* for optical pumping, 2.2 ms *wait* to allow excited population to decay, and 40 ms *storage and retrieval*, during which 795 nm photons are successively stored for $t_{st} = 6$ ns and then recalled.

tral wavelength, 16 ps duration, and 90 mW average power. The FD pulses are sent to a second PPLN crystal that, via SPDC, produces pairs of photons centred at 795.506 nm and 1532.426 nm. Frequency filtering the 795 nm photons with a 6 GHz-bandwidth Fabry-Perot filter (FPF) and the 1532 nm photons with a 9 GHz-bandwidth fiber-Bragg grating (FBG) we obtain frequency uncorrelated pairs. Each 795 nm photon travels through an imbalanced, temperature-stabilized Mach-Zehnder interferometer with 42 cm path-length difference, corresponding to 1.4 ns relative delay. Thus, each photon emerges in a superposition of two temporal modes (early and late), i.e., in a time-bin qubit state [22]. They are then directed into the quantum memory, stored, retrieved, and finally detected by a Si avalanche-photodiode (APD)-based single-photon detector.

All 1532 nm photons are sent through 30 m standard telecommunication fiber to an InGaAs APD-based single-photon detector. As is typically done, the detector is gated to reduce noise. The gate signal could in principle be the SYNC signal derived from each pulse emitted by the pump laser. However, as its repetition rate of 80 MHz by far exceeds the maximum gate frequency of our detector, around 1 MHz, we first AND the SYNC pulses with pulses generated by each Si-APD detection, and then use this low-rate signal to gate the InGaAs-APD. Provided the latter is ready for photon detection (i.e. not deadtime-blocked due to a previous detection), this signal also starts a time-to-digital converter (TDC), which then records the time-difference between the detection events produced by the Si-APD and the InGaAs-APD. This data is used to obtain statistics for single detections of the retrieved 795 nm photons, as well as for detections conditioned on the existence of 1532 nm photons. We emphasize that if an InGaAs APD supporting 80 MHz gate rate had been available [18, 19], then 1532 nm photons could have been detected without the need for *a priori* detection of a 795 nm photon. This simple modification of our setup would have turned the conditional detection of 795 nm photons into detections that are heralded by clicks of the InGaAs APD.

The other main block of our setup is a Ti:Tm:$LiNbO_3$ waveguide that allows storage and retrieval of the 795 nm photons via the atomic frequency comb (AFC) quantum memory protocol [21]. This approach to quantum state storage requires the spectral absorption of an atomic ensemble to be constituted of a series of equally spaced lines with frequency spacing Δ_ν. The interaction between such an AFC and a photon with wavevector k leads to the absorption of the photon and generates a collective excitation in the atomic medium that is described by

$$|\Psi\rangle = \frac{1}{\sqrt{N!}} \sum_{j=1}^{N} c_j e^{i2\pi m_j \Delta_\nu t} e^{-ikz_j} |g_1, \cdots e_j, \cdots g_N\rangle . \quad (1)$$

Here, $|g_j\rangle$ ($|e_j\rangle$) denotes the ground (excited) state of atom j, $m_j\Delta_\nu$ is the detuning of the atom's transition frequency from the photon carrier frequency, z_j its position measured along the propagation direction of the light, and the factor c_j depends on the atom's resonance frequency and position. Due to the presence of different atomic transition frequencies, the excited collective coherence dephases rapidly. However, the particular shape of the absorption line results in the recovery of the collective coherence after storage time $t_{st} = 1/\Delta_\nu$. This can easily be seen from Eq. (1): for $t = 1/\Delta_\nu$ all frequency dependent phase factors are zero (mod 2π). This leads to re-emission of the photon into the original mode and quantum state with maximally 54% efficiency for an optimally implemented AFC. Modifications to the procedure enable recall on demand and up to 100% efficiency [21].

Suitable media in which to implement the AFC protocol are cryogenically cooled rare-earth ion doped crystals [7, 23]. They feature inhomogeneously broadened absorption profiles, often posses long-lived atomic sublevels that can serve as shelving levels for tailoring the AFC through persistent spectral hole burning, and generally have long coherence times on optical and spin transitions. We use the $^3H_6$-$^3H_4$ transition of Tm ions in a single-mode channel waveguide fabricated by Ti indiffusion into the Tm doped surface of a Z-cut $LiNbO_3$ crystal, see Fig. 5.1.2a [20]. To tailor the desired AFC into the inhomogeneously broadened absorption profile, Tm ions with transition frequencies within the comb's troughs are optically pumped via the excited level into long-lived nuclear Zeeman levels, see Fig. 5.1.2b [20, 24]. To achieve

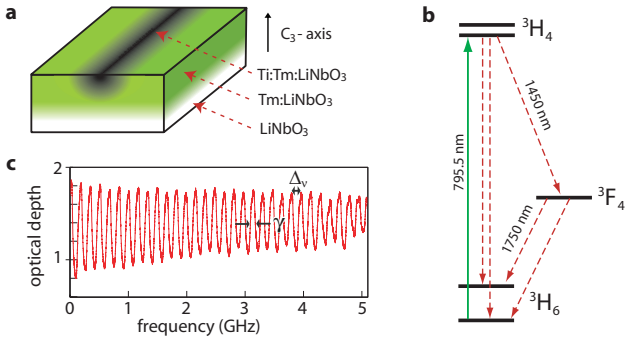


FIG. 5.1.2. **a.** Waveguide geometry: The sample surface is first doped by indiffusing a ≈ 20 nm thick Tm layer yielding a concentration profile of ≈ 6 μm depth with $\approx 10^{20}$ ions per cm^3 surface concentration. Subsequently a 3 μm wide channel waveguide is fabricated by indiffusion of a 40 nm thick vacuum-deposited Ti stripe. AFC preparation light and single photons are coupled in and out of the waveguide with 10% total efficiency by butt-coupling single mode fibers. **b.** Simplified energy level diagram of Tm ions: The optical coherence time of the ^{3}H$_6$-^{3}H$_4$ transition at 3 K is 1.6 μs, and the radiative lifetimes of the ^{3}H$_4$ and ^{3}F$_4$ levels are 82 μs and 2.4 ms, respectively. A 570 G magnetic field splits the ground and excited levels into Zeeman sub-levels. The ground Zeeman level splitting is ~ 83 MHz, and the lifetime of the upper ground level exceeds one second. **c.** 5 GHz-bandwidth AFC: The tooth separation is $\Delta_\nu = 167$ MHz, corresponding to 6 ns storage time. The line-width of the teeth is $\gamma = 83$ MHz.

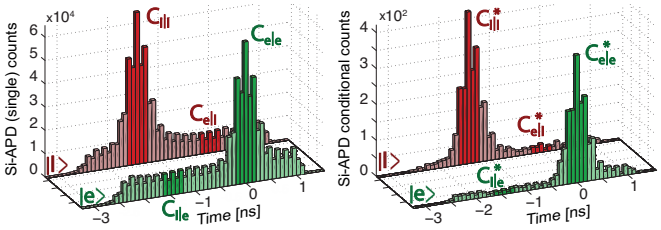


FIG. 5.1.3. Storage of early and late time-bin qubit states in the AFC memory. The left-hand figure depicts the histograms from 180 min of single detections of the retrieved 795 nm photons prepared in early (red) and late (green) qubit states with the highlighted regions marking the relevant detection windows. The right-hand figure shows the detections conditioned on 1532 nm photons for the same states. Without conditioning the fidelities are $\mathcal{F}_e = 0.8652 \pm 0.0006$ and $\mathcal{F}_l = 0.8376 \pm 0.0004$ for the storage of early and late time-bin states, respectively. Correspondingly, with conditioning, the fidelities are $\mathcal{F}_e^* = 0.9505 \pm 0.0058$ and $\mathcal{F}_l^* = 0.9573 \pm 0.0033$.

frequency selective optical pumping we employed a linear side-band chirp technique [11, 25] that allowed us to create a 5 GHz broad grating (matching the spectral width of the 795 nm photons) with tooth spacing of 167 MHz, see Fig. 5.1.2c. This corresponds to a storage time of 6 ns. After each 10 ms-long AFC preparation a 2.2 ms-long wait time allows atoms excited by the optical pumping to decay before photon storage (see Fig. 5.1.1b for the timing per experimental cycle). A set of micro electromechanical switches (MEMS) then open the channel for qubits to enter the memory, and, after recall, direct them towards the Si-APD. We assessed our memory's retrieval efficiency to be $(2\pm0.5)\%$. Taking the 10 dB fibre-to-fibre coupling loss in and out of the waveguide into account, this yields an overall system efficiency of approximately 0.2% [11].

An interesting and useful aspect of photon-echo quantum memory protocols is that they provide a robust tool to manipulate time-bin qubits [26–29]. For example, using the AFC approach, any projection measurement on time-bin qubit states can be performed by superimposing two combs (double AFC) with appropriately chosen relative center frequencies and amplitudes [27]. This leads to two re-emission times that can be set to differ by the temporal mode separation of the qubit to be analyzed (1.4 ns for our experiments). Hence, as a previously absorbed photon is re-emitted by the superimposed combs, early and late temporal modes interfere, allowing the qubit state to be analyzed in the same way as is typically done with an imbalanced Mach-Zehnder interferometer [27]. Double AFC recall will, however, lead to a reduction of the recall efficiency (compared to single recall).

To demonstrate faithful storage and retrieval of quantum states from the memory, we performed projection measurements with various time-bin qubits onto different bases using single (standard) and double AFC schemes as explained before. In all our measurements the average photon number per qubit was 0.1 at the output of the qubit-encoding interferometer. First we generated qubit states that occupy only early $|e\rangle$ or late $|l\rangle$ temporal modes by blocking either the long or short arm of the qubit-encoding interferometer, respectively, and then stored these states in the memory for 6 ns. Fig. 5.1.3 (left) shows single detections (no conditioning) of the retrieved photons as a function of the time difference with respect to the START signal. The dark counts from the Si-APD reduce the signal to noise ratio (SNR) to ~ 5. For an input state $|e\rangle$, we compute the fidelity as $\mathcal{F}_e = C_{e|e}/(C_{e|e} + C_{l|e})$, where, e.g., $C_{l|e}$ denotes the number of detected counts in the late time-bin given $|e\rangle$ was encoded in the qubit at the input. Similarly, we can find $\mathcal{F}_l$, enabling us to calculate the mean fidelity: $\mathcal{F}_{el} = (\mathcal{F}_e + \mathcal{F}_l)/2 = 0.8514 \pm 0.0004$.

On the other hand, conditioning the detections of the retrieved photons on the detection of 1532 nm photons leads to a substantial increase of the SNR to ~ 22, as shown in Fig. 5.1.3 (right). This yields a mean fidelity of $\mathcal{F}_{el}^* = 0.9539 \pm 0.0024$.

Next, qubit states in an equal superposition of early and late temporal modes $\frac{1}{\sqrt{2}}(|e\rangle + e^{i\phi}|l\rangle)$ were produced with ϕ set to zero. Storage and projection measurements

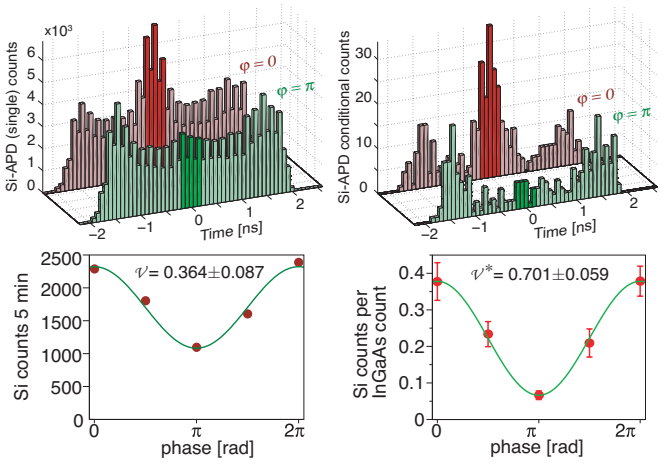


FIG. 5.1.4. Retrieval of qubits created in a superposition of early and late temporal modes. The top left figure presents histograms of single detections of the retrieved 795 nm photons with AFC phase settings of zero (red) and π (green), collected during 80 min. The top right figure shows the same histograms for conditional detections. The highlighted regions mark detection windows used to derive projection probabilities required to calculate fidelities. The lower curves show single and coincidence counts obtained for all phase settings for single detections (left) and conditional detections (right), yielding visibilities of 0.364 ± 0.087 and 0.701 ± 0.059, respectively.

were performed using the double AFC scheme with the relative phase of the two combs (measured w.r.t. the phase introduced by the qubit-encoding interferometer) varied by $\pi/2$ increments. The results for single and conditional detections are given in Fig. 5.1.4. The histograms show the detection statistics for zero and π double AFC phase settings, from which we extract a SNR slightly above 1 for the single, and above 6 for the conditional detection. In the lower part of Fig. 5.1.4 we show the normalized counts for each projection setting for the single and conditional detections. Fitting sinusoidal curves to these we derive visibilities $\mathcal{V}$, which, in turn, yield a fidelity $\mathcal{F} = (1 + \mathcal{V})/2$ for single detections of $\mathcal{F}_\phi = 0.682 \pm 0.020$. For conditional detections we find a significantly larger value of $\mathcal{F}^*_\phi = 0.851 \pm 0.030$. These figures allow establishing an average, single detection fidelity: $\overline{\mathcal{F}} \equiv (\mathcal{F}_{el} + 2\mathcal{F}_\phi)/3 = 0.738 \pm 0.029$. This violates the quantum classical bound [30] of ~ 0.667, thus verifying that our memory outperforms any classical storage protocol. However, it is below the bound of ~ 0.833 for an optimal universal quantum cloner [31]. Harnessing the conditional detection we find $\overline{\mathcal{F}^*} = 0.885 \pm 0.020$. This beats the quantum-classical bound by 10 standard deviations and also violates the optimal universal quantum cloner bound by 2.5 standard deviations.

To conclude, we have demonstrated storage, retrieval, and conditional detection of different time-bin qubit states using a solid-state Ti:Tm:LiNbO3 waveguide quantum memory with average fidelity $\overline{\mathcal{F}^*} = 0.885 \pm 0.020$, which exceeds the relevant classical bounds. Operating the memory in a heralded fashion is readily achievable with high-rate APDs that have recently become commercially available. Despite our memory device's current limitations, namely efficiency, storage time, and preset recall time, the high fidelity and the wide spectral acceptance makes our approach promising for future quantum communication schemes and quantum networks. The $LiNbO_3$ host crystal and the waveguide structure have potential advantages in quantum memory applications such as fast electric field control of collective atomic phase evolution and, due to the resemblance with building blocks of classical integrated optical devices [32], it holds promise for simple integration with existing information technology. Furthermore, the ability to perform projection measurements using a photon-echo memory provides a simple and robust tool that might find use in other applications of quantum information processing.

ACKNOWLEDGEMENTS

We thank C. La Mela and T. Chanelière for helping in the initial stages of this work, V. Kiselyov for technical support, and NSERC, GDC, iCORE (now part of AITF), QuantumWorks, CFI and AET for financial support. D.O. thanks the Carlsberg Foundation and F.B. thanks FQRNT for support.

---

* Current address: Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, 1211 Geneva, Switzerland

[1] H.-J. Briegel *et al.*, Phys. Rev. Lett. **81**, 5932 (1998).
[2] N. Sangouard *et al.*, Rev. Mod. Phys. **83**(1), 33 (2011).
[3] J. Kimble, Nature **453**, 1023 (2008).
[4] P. Kok *et al.*, Rev. Mod. Phys. **79**, 135 (2007).
[5] H. P. Specht *et al.*, Nature **473**, 190 (2011).
[6] H. Tanji *et al.*, Phys. Rev. Lett. **103**, 043601 (2009).
[7] W. Tittel *et al.*, Laser & Phot. Rev. **4**, 244 (2010).
[8] A. I. Lvovsky, B.C. Sanders and W. Tittel, Nature Photonics **3**, 706 (2009).
[9] M. Hosseini *et al.*, Nat. Physics **7**, 794 (2011).
[10] A. G. Radnaev *et al.*, Nat. Physics **6**, 894 (2010).
[11] E. Saglamyurek *et al.*, Nature **469**, 512 (2011).
[12] C. Clausen *et al.*, Nature **469**, 508 (2011).
[13] H. Zhang *et al.*, Nat. Photon. **5**, 628 (2011).
[14] I. Usmani *et al.*, Nat. Commun. **1**, 12 (2010).
[15] K. F. Reim *et al.*, Phys. Rev. Lett. **107**, 053603 (2011).
[16] M. Hedges *et al.*, Nature **465**, 1052 (2010).
[17] K. Akiba *et al.*, New J. Phys. **11**, 013049 (2009).
[18] M. D. Eisaman, et al., **82**(7), 071101 (2011).
[19] ID-Quantique SA, Physics today, **64**, 59 (2011).
[20] N. Sinclair *et al.*, J. Lumin. **130**, 1586 (2010).
[21] M. Afzelius *et al.*, Phys. Rev. A **79**, 052329 (2009).

[22] W. Tittel and G. Weihs, Quant. Inf. Comp., **1**(2), 3 (2001).
[23] C. Thiel, T. Böttger and R. Cone, J. Lumin. **131**, 353 (2011).
[24] C. W. Thiel *et al.*, J. Lumin. **130**, 1598 (2010).
[25] R. R. Reibel *et al.*, J. Lumin. **107**, 103 (2004).
[26] S. A. Moiseev and B. S. Ham, Phys. Rev. A **70**, 063809 (2004).
[27] H. de Riedmatten *et al.*, Nature **456**, 773 (2008).
[28] M. Hosseini *et al.*, Nature **461**, 241 (2009).
[29] S. A. Moiseev and W. Tittel, Phys. Rev. A **82**, 012309 (2010).
[30] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).
[31] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[32] W. Sohler *et al.*, Opt. Photon. News **19**, 24 (2008).

Two-photon interference of weak coherent laser pulses recalled from separate solid-state quantum memories

Jeongwan Jin,[1] Joshua A. Slater,[1] Erhan Saglamyurek,[1] Neil Sinclair,[1] Mathew George,[2] Raimund Ricken,[2] Daniel Oblak,[1] Wolfgang Sohler,[2] and Wolfgang 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] *Department of Physics - Applied Physics, University of Paderborn, Warburger Strasse 100, 33095 Paderborn, Germany*

Quantum memories for light, which allow the reversible transfer of quantum states between light and matter, are central to the development of quantum repeaters, quantum networks, and linear optics quantum computing[1, 2]. Significant progress has been reported in recent years, including the faithful transfer of quantum information from photons in pure and entangled qubit states[3–8]. However, none of these demonstrations confirm that photons stored in and recalled from quantum memories remain suitable for two-photon interference measurements, such as C-NOT gates and Bell-state measurements, which constitute another key ingredient for all aforementioned applications of quantum information processing. Using pairs of weak laser pulses, each containing less than one photon on average, we demonstrate two-photon interference as well as a Bell-state measurement after either none, one, or both pulses have been reversibly mapped to separate thulium-doped titanium-indiffused lithium niobate (Ti:Tm:$LiNbO_3$) waveguides. As the interference is always near the theoretical maximum, we conclude that our solid-state quantum memories, in addition to faithfully mapping quantum information, also preserves the entire photonic wavefunction. Hence, we demonstrate that our memories are generally suitable for use in advanced applications of quantum information processing that require two-photon interference.

When two indistinguishable single photons impinge on a 50/50 beam-splitter (BS) from different input ports, they bunch and leave together by the same output port. This so-called Hong-Ou-Mandel (HOM) effect[9] is due to destructive interference between the probability amplitudes associated with both input photons being transmitted or both reflected, see Fig. 1. Since no such interference occurs for distinguishable input photons, the interference visibility V provides a convenient way to verify that two photons are indistinguishable in all degrees of freedom, i.e. spatial, temporal, spectral, and polarization modes. The visibility is defined as

$$V = (\mathcal{R}_{\max} - \mathcal{R}_{\min})/\mathcal{R}_{\max}, \quad (1)$$

where $\mathcal{R}_{\min}$ and $\mathcal{R}_{\max}$ denote the rate with which photons are detected in the two output ports in coincidence if the incoming photons are indistinguishable and distinguishable, respectively. Consequently, the HOM effect has been employed to characterize the indistinguishability of photons emitted from a variety of sources, including parametric down-conversion crystals[10], trapped neutral atoms[7, 11], trapped ions[12], quantum dots[13], organic molecules[14], nitrogen-vacancy centres in diamond[15, 16], and atomic vapours[17–19]. Furthermore, two-photon interference is at the heart of linear optics Bell-state measurements[20], and, as such, has already enabled experimental quantum dense coding, quantum teleportation, and entanglement swapping[21]. However, to date, the possibility to perform Bell-state measurements with photons that have previously been stored in a quantum memory, as required for advanced applications of quantum information processing, has not yet been established. For these measurements to succeed, photons need to remain indistinguishable in all degrees of freedom, which is more restrictive than the faithful recall of encoded quantum information. Indeed, taking into account that photons may or may not have been stored before the measurement, this criterion amounts to the requirement that a quantum memory preserves a photon's wavefunction during storage. Similar to the case of photon sources, the criterion of indistinguishability is best assessed using HOM interference, provided single-photon detectors are employed.

Our experimental setup is depicted in Fig. 5.2.2. We employ solid-state quantum memories, more precisely thulium-doped lithium-niobate waveguides in conjunction with the atomic frequency comb (AFC) quantum memory protocol[22], which have shown great promise for advanced applications of quantum information processing[4, 5]. We then interfere various combinations of recalled and non-stored (i.e. directly transmitted) pulses on a 50/50 BS (HOM-BS). When using single photon Fock states at the memory inputs, the HOM visibility given in Eq. (1) theoretically reaches 100% as illustrated in Fig. 5.2.1. However, with phase incoherent laser pulses obeying Poissonian photon-number statistics, as in our demonstration, the maximally achievable visibility is 50%[23], irrespective of the mean photon number (see Supplementary Information). Nevertheless, attenuated laser pulses are perfectly suitable for assessing the effect of our quantum memories on the photonic wavefunction. Any reduction of indistinguishability due to

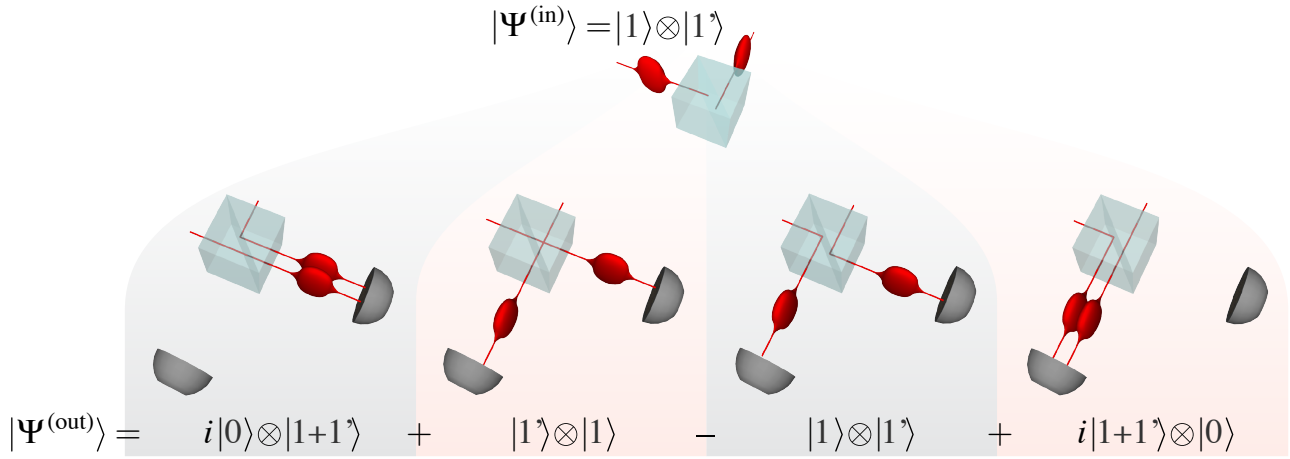


FIG. 5.2.1. Illustration of HOM-interference in the case of single photons at BS input $|\psi^{(\mathrm{in})}\rangle = |1, 1'\rangle$, where the prime on the latter input indicates the possibility to distinguish that input photon from the other in some degree of freedom e.g. by being polarized orthogonally. The four possible paths of the photons are illustrated, together with their corresponding output states. If the input photons are indistinguishable with respect to all degrees of freedom we can ignore the primes in the output states and the paths shown in the two central pictures are identical and, due to the different signs, thus cancel. This leaves in the output state $|\psi^{(\mathrm{out})}\rangle$ only the possibilities in which photons bunch. For distinguishable photons, e.g. having orthogonal polarizations, all paths are distinguishable and all terms remain in $|\psi^{(\mathrm{out})}\rangle$.

storage causes a reduction of visibility, albeit from maximally 50%. This approach extends the characterization of quantum memories using attenuated laser pulses[24] from assessing the preservation of quantum information during storage to assessing the preservation of the entire wavefunction, and from first- to second-order interference.

We first deactivate both quantum memories (see Methods), to examine the interference between directly transmitted pulses, and thereby establish a reference visibility for our experimental setup. We set the mean photon number per pulse before the memories to 0.6, i.e. to the single-photon level. Using the wave plates, we rotate the polarizations of the pulses at the two HOM-BS inputs to be parallel (indistinguishable) or orthogonal (distinguishable) and in both cases record the coincidence detection rates of the detectors at the HOM-BS outputs. Employing Eq. (1) we find a visibility of $(47.9 \pm 3.1)\%$.

Subsequently, we activate memory a while keeping memory b off, and adjust the timing of the pulse preparation so as to interfere a recalled pulse from the active memory with a directly transmitted pulse from the inactive memory (see Methods). Pulses are stored for 30 ns in memory a, and the mean photon number per pulse at the quantum memory input is 0.6. Taking the limited storage efficiency of $\approx 1.5\%$ and coupling loss into account, this results in 3.4×10^{-4} photons per pulse at the HOM-BS inputs. As before, changing the pulse polarizations from mutually parallel to orthogonal, we find $V = (47.7 \pm 5.4)\%$, which equals our reference value within the measurement uncertainties.

As the final step, we activate both memories to test the feasibility of two-photon interference in a quantum-repeater scenario. We note that in a real-world implementation, memories belonging to different network nodes are not necessarily identical in terms of material properties and environment. This is captured by our setup where the two Ti:Tm:$LiNbO_3$ waveguides feature different optical depths and experience different magnetic fields (see Fig. 5.2.2 and Supplementary Information). To balance the ensuing difference in memory efficiency we set the mean photon number per pulse before the less efficient and more efficient memories to 4.6 and 0.6, respectively, so that, as before, the mean photon numbers are 3.4×10^{-4} at both HOM-BS inputs. With the storage time of both memories set to 30 ns, we find $V = (47.2 \pm 3.4)\%$, in excellent agreement with the values from the previous measurements. The consistently high visibilities, compiled in the first column of Table 5.2.1, hence confirm that our storage devices do not introduce any degradation of photon indistinguishability during the reversible mapping process, and that two-photon interference is feasible with photons recalled from separate quantum memories, even if the memories are different.

We now investigate in greater detail the change in coincidence count rates as photons gradually change from being mutually indistinguishable to completely distinguishable w.r.t. each degree of freedom accessible for change in single-mode fibres, i.e. polarization, temporal, and spectral modes (see Methods). To acquire data more efficiently we increase the mean number of photons per pulse at the memory input to between 10 and 50 (referred to as few-photon-level measurements). However, the mean photon number at the HOM-BS remains below

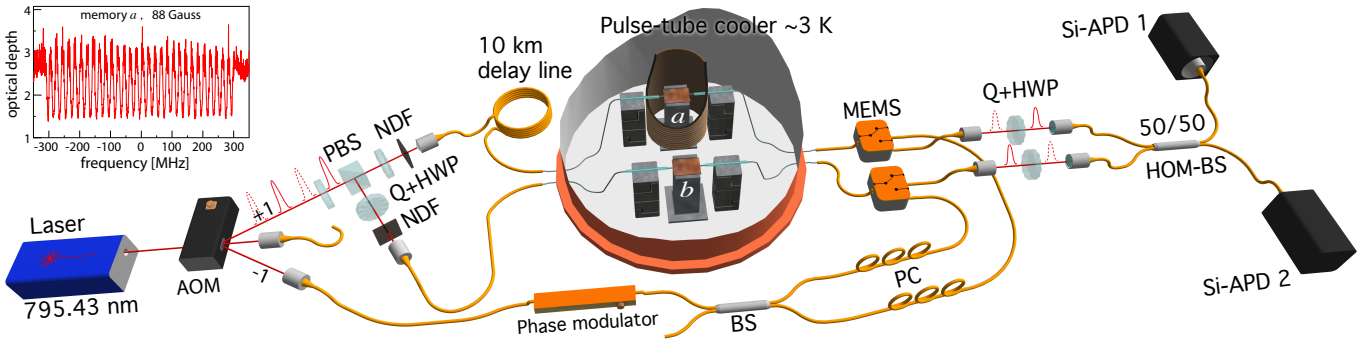


FIG. 5.2.2. **Experimental setup.** Light from a 795.43 nm wavelength CW laser passes through an acousto-optic modulator (AOM) driven by a sinusoidally varying signal. The first negative refraction order is fibre coupled into a phase modulator and, via a beam-splitter (BS), two polarization controllers (PCs) and two micro-electromechanical switches (MEMS), injected from the back into two Ti:Tm:$LiNbO_3$ waveguides (labelled a and b) cooled to 3 K [30]. Waveguide a is placed inside a superconducting solenoid. Using a linear frequency-chirping technique[4] we tailor AFCs with 600 MHz bandwidth and a few tens of MHz peak spacing, depending on the experiment, into the inhomogeneously broadened absorption spectrum of the thulium ions, as shown for crystal a in the inset. After 3 ms memory preparation time and 2 ms wait time we store and recall probe pulses during 3 ms. The 8 ns long probe pulses with $\approx$ 50 MHz Fourier-limited bandwidth are derived from the first positive diffraction order of the AOM output at a repetition rate of 2.5-3 MHz. Each pulse is divided into two spatial modes by a half-wave plate (HWP) followed by a polarizing beam-splitter (PBS). All pulses are attenuated by neutral-density filters (NDFs) and coupled into optical fibres and injected from the front into the Ti:Tm:$LiNbO_3$ waveguides. After exiting the memories (i.e. either after storage, or after transmission), the pulses pass quarter- and half-wave plates used to control their polarizations at the 50/50 BS (HOM-BS) where the two-photon interference occurs. Note that, to avoid first-order interference, pulses passing through memory a propagate through a 10 km fibre to delay them w.r.t. the pulses passing through memory b by more than the laser coherence length. Finally, they are detected by two single-photon detectors (actively quenched silicon avalanche photodiodes, Si-APDs) placed at the outputs of the beam-splitter, and coincidence detection events are analyzed with a time-to-digital convertor (TDC) and a computer.

one. Example data plots are shown in Fig. 5.2.3, while the complete set of plots is supplied in the Supplementary Information Figs. 3-5.

In Fig. 5.2.3a we show the coincidence counts rates as a function of the polarization of the recalled pulse for the case of one active memory. The visibilities for all configurations (i.e. zero, one, or two active memories) extracted from fits to the experimental data are listed in column 2 of Table 5.2.1. They are – as in the case of single-photon-level inputs – equal to within the experimental uncertainty.

Next, in Fig. 5.2.3b, we depict the coincidence count rates as a function of the temporal overlap (adjusted by the timing of the pulse generation) for the two-memory configuration. Column 3 of Table 5.2.1 shows the visibilities extracted from Gaussian fits to the data, reflecting the temporal profiles of the probe pulses, for all configurations. Within experimental uncertainty, they are equal to each other. Alternatively, in the single-memory configuration, we also change the temporal mode overlap by adjusting the storage time of the pulse mapped to the quantum memory. Again the measured visibility of $V = (44.4 \pm 6.9)\%$ (see Fig. 5.2.3c) is close to the theoretical maximum.

Finally, we vary the frequency difference between the two pulses (see Methods) to witness two-photon interference w.r.t. spectral distinguishability. For this measurement, we consider only the configurations in which neither, or a just single memory is active. In both cases the visibilities, listed in the last column of Table 5.2.1, are around 43%. While this is below the visibilities found previously, for reasons discussed in the Supplementary Information, the key observation is that the quantum memory does not affect the visibility.

As stated in the introduction, Bell-state measurements (BSM) with photonic qubits recalled from separate quantum memories are key ingredients for advanced applications of quantum communication. To demonstrate this important element, we consider the asymmetric (and arguably least favourable) configuration in which only one of the qubits is stored and recalled. Appropriately driv-

TABLE 5.2.1. Experimental two-photon interference visibilities (%) for different degrees of freedom

Storage	Single-photon level	Few-photon level		
configuration	Polarization	Polarization	Temporal	Spectral
No-storage	47.9 ± 3.1	51.0 ± 5.6	42.4 ± 2.3	43.7 ± 1.7
Single-storage	47.7 ± 5.4	55.5 ± 4.1	47.6 ± 3.0	42.4 ± 3.5
Double-storage	47.2 ± 3.4	53.1 ± 5.3	46.1 ± 3.2	N. A.

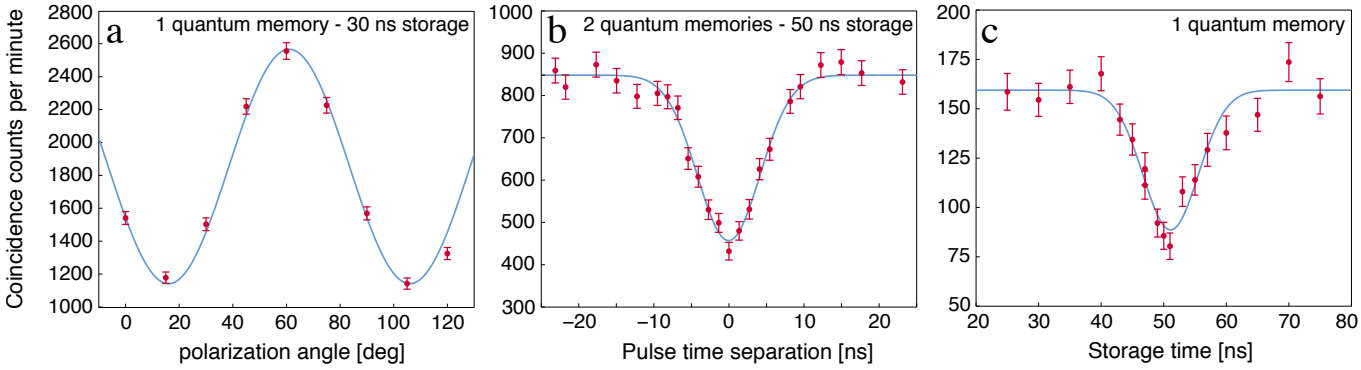


FIG. 5.2.3. HOM interference plot examples for one or two active memory configurations (as labelled). a) Varying mutual polarization difference. b) Varying temporal overlap by changing timing of pulse generation. c) Varying temporal overlap by changing storage time. The acquisition time per data point is 60 s in a,b and 120 s in c.

ing the AOM in Fig. 5.2.2, we prepare the states $|\Psi_1\rangle$ and $|\Psi_2\rangle$, which describe time-bin qubits[21] of the form $|e\rangle$, $|l\rangle$, $\frac{1}{\sqrt{2}}(|e\rangle + |l\rangle)$, or $\frac{1}{\sqrt{2}}(|e\rangle - |l\rangle)$, where e and l, respectively, label photons in early or late temporal modes, which are separated by 25 ns. The qubits are directed to the memories of which only one is activated. The mean photon number of the qubit that is stored is set to 0.6, yielding a mean photon number of both qubits at the HOM-BS input of 6.7×10^{-4}. We ensure to overlap pulses encoding the states $|\Psi_1\rangle$ and $|\Psi_2\rangle$ at the HOM-BS and count coincidence detections that correspond to a projection onto the $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|e\rangle|l\rangle - |l\rangle|e\rangle)$ Bell state. This projection occurs if the two detectors click with 25 ns time difference[21]. Because $|\psi^-\rangle$ is antisymmetric w.r.t. any basis, the count rate is expected to reach a minimum value $\mathcal{R}_{\|}$ if the two input pulses are prepared in equal states, and a maximum value $\mathcal{R}_{\perp}$ if prepared in orthogonal states. Accordingly, we define an error rate that quantifies the deviation of the minimum count rate from its ideal value of zero:

$$e \equiv \frac{\mathcal{R}^{\|}}{\mathcal{R}^{\|} + \mathcal{R}^{\perp}}\,. \tag{2}$$

First, choosing to encode $|\Psi_1\rangle$ and $|\Psi_2\rangle$ in states $|e\rangle$ and $|l\rangle$ we obtain the error rate $e_{e/l}^{(\mathrm{exp})} = 0.039 \pm 0.037$, which is near the theoretical value of $e_{e/l}^{(\mathrm{QM})} = 0$ (see the Supplementary Information for derivations of the theoretical values and bounds). In addition it clearly violates the lower bound $e_{e/l}^{(\mathrm{CM})} = 0.33$ that can be obtained for a Bell-state measurement on two qubits of which one is recalled from a classical memory (CM). Note that values for $e_{e/l}^{(\mathrm{QM})}$ and $e_{e/l}^{(\mathrm{CM})}$ are independent of whether $|e\rangle$ and $|l\rangle$ qubits are encoded into single photons or attenuated laser pulses. Next, using instead the states $|+\rangle \equiv \frac{1}{\sqrt{2}}(|e\rangle + |l\rangle)$, and $|-\rangle \equiv \frac{1}{\sqrt{2}}(|e\rangle - |l\rangle)$ we measure $e_{+/-}^{(\mathrm{exp})} = 0.287 \pm 0.020$, which again only slightly exceeds the lowest possible value for attenuated laser pulses of $e_{+/-}^{(\mathrm{att,QM})} = 0.25$. The crucial observation is once more that $e_{+/-}^{(\mathrm{exp})}$ violates both the lower bound for qubits encoded into single photons $e_{+/-}^{(\mathrm{sing,CM})} = 0.33$ and attenuated laser pulses $e_{+/-}^{(\mathrm{att,CM})} = 0.417$ when these have at one input of the HOM-BS been recalled from a classical memory.

Our demonstrations show that solid-state AFC quantum memories are suitable for two-photon interference experiments, even in the general case of storing the two photons an unequal number of times. With improved system efficiency[25] and multi-mode storage supplemented by read-out on demand, which can be achieved either by selecting the storage time of photons stored at different times[27], or by selecting the frequency of recalled photons from many possible frequency bins occupied by simultaneously stored photons[26], such memories can be used as synchronization devices in multi-photon experiments. This will allow increasing the number of photons that can be harnessed simultaneously for quantum information processing beyond the current limit of eight[28]. A subsequent goal is to develop workable quantum repeaters or, more generally, quantum networks, for which longer storage times are additionally needed. Depending on the required value, which may range from a hundred micro-seconds[29] to seconds[1], this may be achieved by storing quantum information in optical coherence, or it may require mapping of optical coherence onto spin states[22].

METHODS

Memory operation and properties. A quantum memory is said to be activated when we configure the MEMS to allow the optical pumping light to reach the waveguide during the preparation stage and thus tailor an AFC in the inhomogeneously broadend absorption spectrum of thulium ions (see Fig. 5.2.2). If the optical

pumping is blocked, the memory is said to be deactivated and light entering the waveguide merely experiences constant attenuation over its entire spectrum. If a memory is activated, an incident photon is mapped onto a collective excitation of thulium ions in the prepared AFC and subsequently re-emitted at a time given by the inverse of the comb tooth spacing[22], i.e., $t = 1/\Delta$ (see Fig. 5.2.2). In all cases, we adjust the mean photon number at the memory inputs so that mean photon numbers are equal at the HOM-BS inputs. This is required for achieving maximum visibility with attenuated laser pulses (see Supplementary Information).

The two Ti:Tm:$LiNbO_3$ waveguides are fabricated identically but differ in terms of overall length, yielding optical depths of 2.5 for memory a and 3.2 for memory b. As shown in Figure 1, memory a is placed at the centre of a solenoid in a uniform magnetic field, while memory b is placed outside the solenoid and thus experiences only a much weaker stray field. Therefore it is not possible to achieve the optimal efficiency for both memories at the same time (see Supplementary Information).

Changing degrees of freedom. a) The polarization degree is easily adjusted using the free-space half- and quarter-wave plate set at each HOM-BS input. For our measurements we rotate the half-wave plate in steps of either 45 or 7.5 degrees. **b)** The temporal separation δt between a pulse arriving at one of the HOM-BS inputs and the next pulse in the train arriving at the other input can be expressed as $\delta t = \{nl/c\} \bmod \delta t_r$, where n is the refractive index of the fibres, $l \approx 10$ km is the path-length difference for pulses interacting with memory a and b, and δt_r is the repetition period of the pulse train from the AOM, which is set in the range of 350-400 ns. As we can change δt_r with 10 ps precision, we can tune δt on the ns scale. **c)** For the storage time scan, the recall efficiency decreases with storage time due to decoherence. Hence, we balance the mean photon number per pulse for stored and transmitted pulses for each storage time. **d)** Finally, to change the spectral overlap of the pulses input to the HOM-BS we can utilize that these pulses were generated at different times in the AOM and thus we can chose their carrier frequencies independently. We interchangeably drive the AOM by frequencies ν_a and ν_b and thus create two interlaced trains of pulses with different frequencies. By adjusting the pulse timing we can ensure that the pulses overlapped at the HOM-BS belong to different trains and thus have a spectral overlap given by $\delta\nu = \nu_a - \nu_b$. Due to the limited bandwidth of the AOM we are only able to scan $\delta\nu$ by 100 MHz, which, when compared to the 50 MHz pulse bandwidth, is not quite sufficient to make the pulses completely distinguishable. To achieve complete distinguishability, we supplement with a measurement using orthogonal polarizations at the inputs (see Supplementary Information).

Preparing states for Bell-state measurement. For the Bell-state projection measurement we interchangeably prepare the time-bin qubits in either $|e\rangle$ or $|l\rangle$, or in $\frac{1}{\sqrt{2}}(|e\rangle + |l\rangle)$ and $\frac{1}{\sqrt{2}}(|e\rangle - |l\rangle)$ by setting the relative phase and intensity of the AOM drive signal. Adjusting the timing of the pulse preparation we ensure that qubits in different states overlap at the HOM-BS.

ACKNOWLEDGEMENTS

The authors thank Vladimir Kiselov for technical support and NSERC and AITF for financial support. J.A.S. thanks the Killam Trusts and D.O. thanks the Carlsberg Foundation for financial support.

References

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

[2] Kok, P. *et al.* Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.* **79**, 135–174 (2007).

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

[4] Saglamyurek, E. *et al.* Broadband waveguide quantum memory for entangled photons. *Nature* **469**, 512–515 (2011).

[5] Clausen, C. *et al.* Quantum storage of photonic entanglement in a crystal. *Nature* **469**, 508–511 (2011).

[6] Zhang, H. *et al.* Preparation and storage of frequency-uncorrelated entangled photons from cavity-enhanced spontaneous parametric downconversion. *Nat Photon* **5**,

[7] Specht, H. P. *et al.* A single-atom quantum memory. *Nature* **473**, 190–193 (2011).

[8] England, D. G. *et al.* High-fidelity polarization storage in a gigahertz bandwidth quantum memory. *Journal of Physics B: Atomic, Molecular and Optical Physics* **45**, 124008 (2012).

[9] 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).

[10] Kaltenbaek, R., Blauensteiner, B., Żukowski, M., Aspelmeyer, M. & Zeilinger, A. Experimental interference of independent photons. *Phys. Rev. Lett.* **96**, 240502 (2006).

[11] Beugnon, J. *et al.* Quantum interference between two single photons emitted by independently trapped atoms. *Nature* **440**, 779–782 (2006).

[12] Maunz, P. *et al.* Quantum interference of photon pairs from two remote trapped atomic ions. *Nat Phys* **3**, 538–541 (2007).

[13] Patel, R. B. *et al.* Two-photon interference of the emission from electrically tunable remote quantum dots. *Nat Photon* **4**, 632–635 (2010).

[14] Lettow, R. *et al.* Quantum interference of tunably indistinguishable photons from remote organic molecules. *Phys. Rev. Lett.* **104**, 123605 (2010).

[15] Bernien, H. *et al.* Two-photon quantum interference from separate nitrogen vacancy centers in diamond. *Phys. Rev. Lett.* **108**, 043604 (2012).

[16] Sipahigil, A. *et al.* Quantum interference of single photons from remote nitrogen-vacancy centers in diamond. *Phys. Rev. Lett.* **108**, 143601 (2012).

[17] Felinto, D. *et al.* Conditional control of the quantum states of remote atomic memories for quantum networking. *Nat Phys* **2**, 844–848 (2006).

[18] Chanelière, T. *et al.* Quantum interference of electromagnetic fields from remote quantum memories. *Phys. Rev. Lett.* **98**, 113602 (2007).

[19] Chen, Y.-A. *et al.* Memory-built-in quantum teleportation with photonic and atomic qubits. *Nat Phys* **4**, 103–107 (2008).

[20] Weinfurter, H. Experimental bell-state analysis. *Europhysics Letters* **25**, 559–564 (1994).

[21] Tittel, W. & Weihs, G. Photonic entanglement for fundamental tests and quantum communication. *Quant. Inf. Comp.* **1**, 3–56 (2001).

[22] Afzelius, M., Simon, C., de Riedmatten, H. & Gisin, N. Multimode quantum memory based on atomic frequency combs. *Phys. Rev. A* **79**, 052329 (2009).

[23] Mandel, L. Photon interference and correlation effects produced by independent quantum sources. *Phys. Rev. A* **28**, 929–943 (1983).

[24] de Riedmatten, H., Afzelius, M., Staudt, M. U., Simon, C. & Gisin, N. A solid-state light-matter interface at the single-photon level. *Nature* **456**, 773–777 (2008).

[25] Afzelius, M. & Simon, C. Impedance-matched cavity quantum memory. *Phys. Rev. A* **82**, 022310 (2010).

[26] Sinclair, N. *et al.* Quantum repeaters using frequency-multiplexed quantum memories. QCMC 2012 Book of Abstracts, 84, (2012). Manuscript in preparation.

[27] Afzelius, M. *et al.* Demonstration of atomic frequency comb memory for light with spin-wave storage. *Phys. Rev. Lett.* **104**, 040503 (2010).

[28] Yao, X.-C. *et al.* Observation of eight-photon entanglement. *Nat Photon* **6**, 225–228 (2012).

[29] Munro, W. J., Harrison, K. A., Stephens, A. M., Devitt, S. J. & Nemoto, K. From quantum multiplexing to high-performance quantum networking. *Nat Photon* **4**, 792–796 (2010).

[30] Sinclair, N. *et al.* Spectroscopic investigations of a ti:tm:linbo3 waveguide for photon-echo quantum memory. *Journal of Luminescence* **130**, 1586 – 1593 (2010).

Broadband Waveguide Quantum Memory for Entangled Photons

Erhan Saglamyurek,[1] Neil Sinclair,[1] Jeongwan Jin,[1] Joshua A. Slater,[1] Daniel Oblak,[1]
Félix Bussières,[1,*] Mathew George,[2] Raimund Ricken,[2] Wolfgang Sohler,[2] and Wolfgang Tittel[1]

[1] *Institute for Quantum Information Science, and Department of Physics & Astronomy, University of Calgary, 2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada*
[2] *Department of Physics - Applied Physics, University of Paderborn, Warburger Str. 100, 33095 Paderborn, Germany*

The reversible transfer of quantum states of light into and out of matter constitutes an important building block for future applications of quantum communication: it will allow the synchronization of quantum information [1], and the construction of quantum repeaters [2] and quantum networks [3]. Much effort has been devoted to the development of such quantum memories [1], the key property of which is the preservation of entanglement during storage. Here we report the reversible transfer of photon–photon entanglement into entanglement between a photon and a collective atomic excitation in a solid–state device. Towards this end, we employ a thulium-doped lithium niobate waveguide in conjunction with a photon-echo quantum memory protocol [4], and increase the spectral acceptance from the current maximum [5] of 100 Megahertz to 5 Gigahertz. We assess the entanglement-preserving nature of our storage device through Bell inequality violations [6] and by comparing the amount of entanglement contained in the detected photon pairs before and after the reversible transfer. These measurements show, within statistical error, a perfect mapping process. Our broadband quantum memory complements the family of robust, integrated lithium niobate devices [7]. It simplifies frequency-matching of light with matter interfaces in advanced applications of quantum communication, bringing fully quantum-enabled networks a step closer.

Quantum communication is founded on the encoding of information, generally referred to as quantum information, into quantum states of light [6]. The resulting applications of quantum physics at its fundamental level offer cryptographic security through quantum key distribution without relying on unproved mathematical assumptions [8] and allow for the disembodied transfer of quantum states between distant places by means of quantum teleportation [6]. Reversible mapping of quantum states between light and matter is central to advanced applications of quantum communication such as quantum repeaters [2] and quantum networks [3], in which matter constitutes nodes that hold quantum information until needed, and thereby synchronize the information flow through the communication channel or network. Furthermore, such a quantum interface allows the generation of light–matter entanglement through the mapping of one of two entangled photons into matter. To determine whether and how different physical systems can be entangled, and to localize the fundamental or technological boundaries where this fascinating quantum link breaks down, are central goals in quantum physics and have received much attention over the past decades [6].

The reversible light–matter interface can be realized through the direct transfer of quantum states from light onto matter and back, or through the generation of light–matter entanglement followed by teleportation of quantum information from an externally provided photon into matter, and eventually back. Experimental capabilities have advanced rapidly over the past years and quantum state transfer between light and atomic vapour [9–13], solid–state ensembles [4,14], or single absorbers [15], as well as the generation of light–matter entanglement through the absorption of photons [16–18], or the emission of photons from atomic ensembles [19–21] or single emitters [22, 23] have all been reported.

For quantum memory to become practical, it is important to reduce the complexity of experimental implementations, and the recent addition of rare-earth-ion-doped crystals [4,14] to the set of storage materials has been a valuable step towards this goal. The promise of such crystals is further enhanced through potentially long storage times–up to several seconds in $Pr:Y_2SiO_5$ [24]. In addition, given the large inhomogeneous broadening of optical zero-phonon lines, up to 100 Gigahertz (GHz), rare-earth-ion-doped crystals in principle offer storage of photons with less than 100-picosecond duration when being used in conjunction with a suitable quantum memory protocol [4]. Yet, the reversible state transfer between light and solid–state devices has so far not been shown to preserve entanglement. This is largely due to the limited spectral bandwidth of current implementations, 100 Megahertz (MHz) at most [5], which is orders of magnitude smaller than that of entangled photon pairs generated in the widely used process of spontaneous parametric down-conversion [6]. In this work, we approach the problem from both ends: we increase the acceptance bandwidth of our storage device to 5 GHz and narrow the bandwidths of our entangled photons to similar values. Furthermore, by using a wave-guiding storage medium, we move fundamental quantum memory research further towards application. The layout of our experiment is depicted in Fig. 5.3.1. Short pulses of 523-nm wavelength light travel through an unbalanced interferometer. For sufficiently small pulse energies, subsequent spontaneous parametric down-conversion yields, to a good approxima-

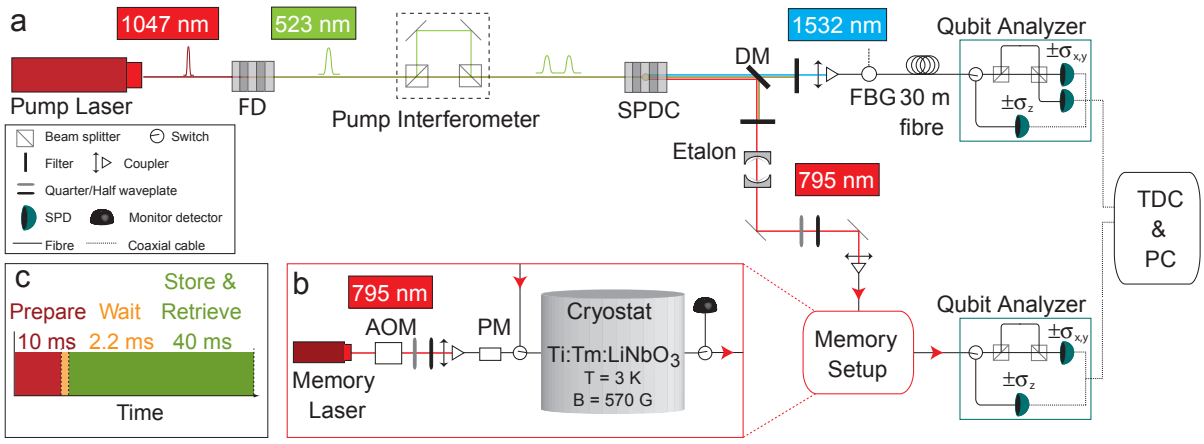


FIG. 5.3.1. **Schematics of the experimental set-up: a**. Generating and measuring entanglement. Six-picosecond-long pump laser pulses (1,047.328 nm wavelength, 80 MHz repetition rate) are frequency doubled (FD) in a periodically poled lithium niobate (PPLN) crystal. Each resulting 16-ps-long pulse (523.664-nm wavelength, 90 mW average power) is coherently split into two by the unbalanced pump interferometer, featuring a 1.4-ns travel-time difference. Spontaneous parametric down-conversion (SPDC) in a second PPLN crystal followed by frequency filtering using an etalon and a fibre Bragg grating (FBG) (bandwidths of 6 GHz and 9 GHz, respectively), yields maximally entangled pairs of photons centred at 795.506-nm and 1,532.426-nm wavelength (DM, dichroic mirror). The 1,532-nm photon travels through a 30-m telecommunication fibre, and the 795-nm photon is either stored in the memory or sent through a fibre delay line (not pictured). To characterize the bi-photon state, we use qubit analysers consisting of delay lines or unbalanced interferometers connected to single-photon detectors. Detection events are collected with a time-to-digital converter (TDC) connected to a personal computer (PC). All interferometers are phase-locked to stable reference lasers (not shown). **b**. Memory set-up. The 795.506-nm continuous-wave memory laser beam is intensity- and phase/frequency-modulated using an acousto-optic modulator (AOM) and a phase modulator (PM). The waveguide is cooled to 3 K and exposed to a 570-G magnetic field aligned with the crystal's C_3-axis. Waveplates allow adjusting the polarization of the beam to the waveguide's transverse magnetic (TM) mode, and optical switches combine and separate the optical pump beam and the 795-nm photons. **c**. Timing sequence. We use three continuously repeated phases: the 10 ms "prepare" phase for optical pumping, the 2.2-ms "wait" phase, which ensures stored photons are not polluted by fluorescence from the excited state, and the 40-ms "store and retrieve" phase, during which many 795-nm photons are successively stored in the waveguide and recalled after 7 ns.

tion, individual pairs of photons, centred at wavelengths around 795 nm and 1,532 nm, in the time-bin entangled qubit state [25]:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|e,e\rangle + |l,l\rangle\right) \qquad (1)$$

Here, $|e\rangle$ and $|l\rangle$ denote early and late temporal modes and replace the usual spin-down and spin-up notation for spin-half particles. More specifically, $|i,j\rangle$ denotes a quantum state in which the 795-nm photon has been created in the temporal mode i, and the 1,532-nm photon has been created in the temporal mode j. We point out that, owing to the spectral filtering, our source generates frequency-uncorrelated entangled photons at wavelengths that match the low-loss windows of free-space and standard telecommunication fibre. It can thus be readily used in real-world applications of quantum communication that involve quantum teleportation and entanglement swapping.

The 1,532-nm photon is directed to a qubit analyser. It consists of either a fibre delay line followed by a single-photon detector that monitors the photon's arrival time, or a fibre-optical interferometer that is unbalanced in the same way as the pump interferometer, followed by single-photon detectors. The role of the delay line is to perform projection measurements of the photon's state onto early and late qubit states. Alternatively, the interferometer enables projections onto equal superpositions of early and late modes [25]. Using the language of spin-half systems, this corresponds to projections onto σ_z and, for appropriately chosen phases, σ_x and σ_y, respectively.

The 795-nm photon is transmitted to the quantum memory where its state –specifically that it is entangled with the 1,532-nm photon– is mapped onto a collective excitation of millions of thulium ions. Some time later, the state is mapped back onto a photon that exits the memory through a fibre in well-defined spatio-temporal modes and is probed by a second qubit analyser.

To reversibly map the 795-nm photon onto matter, we use a photon-echo quantum memory protocol based on atomic frequency combs (AFC) [4]. It is rooted in the interaction of light with an ensemble of atomic absorbers (so far rare-earth-ion-doped crystals cooled to cryogenic temperatures) with an inhomogeneously broadened ab-

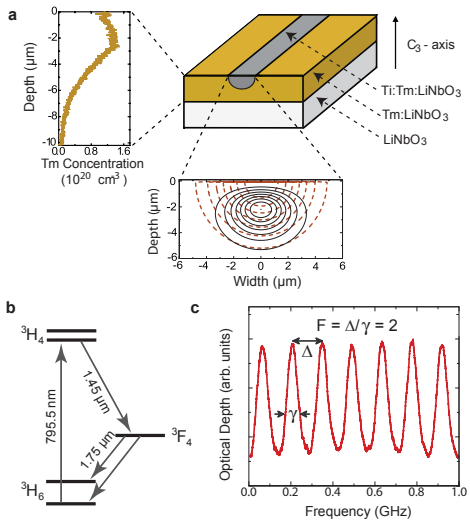


FIG. 5.3.2. **The storage medium: a**. Waveguide geometry. The measured thulium (Tm) concentration profile is given on the left and the calculated intensity distribution of the fundamental TM-mode at the 795-nm wavelength is shown below. Iso-intensity lines are plotted corresponding to 90%, 87.5%, 75% and so on of the maximum intensity. **b**. Simplified energy level diagram of thulium ions. The optical coherence time of the $^3H_6 \leftrightarrow {}^3H_4$ transition at 3 K is 1.6 μs, the radiative lifetimes of the $^3H_4$ and $^3F_4$ levels are 82 μs and 2.4 ms, respectively, and the branching ratio from the $^3H_4$ to the $^3F_4$ level is 44%. Upon application of a magnetic field of 570 G, the ground and excited levels split into magnetic sublevels with lifetimes exceeding one second [27].**c**. Atomic frequency comb. The bandwidth of our AFC is 5 GHz (shown here is a 1-GHz broad section). The separation between the teeth is $\Delta \approx 143$ MHz, resulting in 7 ns storage time. The line width of the peaks is $\gamma \approx 75$ MHz, yielding a finesse $F = 2$, as expected for the sinus-type comb.

sorption line that has been tailored into a series of equally spaced absorption peaks (see Fig. 5.3.2). The absorption of a single photon leads to a collective excitation shared by many atoms. Owing to the particular shape of the tailored absorption line, the excited collective coherence rapidly dephases and repeatedly recovers after multiples of the storage time T_s. This results in the re-emission of a photon in the state encoded into the original photon.

In our implementation the moment of photon re-emission is predetermined by the spacing of the teeth in the comb, $T_s = 1/\Delta$, and the storage process can be described as arising from the linear response of an optical filter made by spectral hole burning. Yet, readout on demand can be achieved by temporarily mapping the optically excited coherence onto ground-state coherence where the comb spacing is smaller or the comb structure is washed out [4], or by combining the AFC protocol with controlled reversible inhomogeneous broadening of each absorption line, similar to the storage mechanism used in another photon-echo quantum memory protocol [1].

Our storage device, a Ti:Tm:$LiNbO_3$ optical waveguide cooled to 3 K, is detailed in Fig. 5.3.2. It was previously characterized to establish its suitability as a photon-echo quantum memory material [26]. It combines interesting properties from the specific rare-earth element (795-nm storage wavelength), the host crystal (allowing for controlled dephasing and rephasing by means of electric fields), and from the wave-guiding structure (ease-of-use). Lithium niobate waveguides have also been doped with neodymium, praseodymium and erbium [7], and we conjecture that other rare-earth ions could also be used. This could extend the properties of $LiNbO_3$ and allow an integrated approach to other storage wavelengths, ions with different level structures, and so on.

To generate the AFC, we use a sideband-chirping technique (see Supplementary Information) to transfer atomic population between magnetic sublevels and create troughs and peaks in the inhomogeneously broadened absorption line. They form a 5-GHz-wide comb with tooth spacing of 143 MHz, setting the storage time to 7 ns. The system efficiency in our implementation is currently about 0.2%. This is in part due to the 90% fibre-to-waveguide input and output coupling loss, which we attribute to imperfect mode overlap. In addition, owing to the specific level structure of thulium under current experimental conditions, the finesse of the comb in the broadband approach is two, which limits the memory efficiency to about 10%. However, imperfections in the creation of the comb decrease this efficiency to around 2%. The system efficiency can be increased by improving the spectral tailoring of the AFC, and triggering photon re-emission in the backward direction. By also optimizing the mode overlap, we anticipate that it could reach approximately 15%. Furthermore, if the two long-lived atomic levels between which population is transferred during the optical pumping procedure (in our case the two magnetic ground states; see Fig. 5.3.2) are spaced by more than the storage bandwidth, the memory efficiency can theoretically reach unity (see Supplementary Information).

To assess the quantum nature of our light–matter interface, we first make projection measurements with the 795 nm photons and the 1532 nm photons onto time-bin qubit states characterized by Bloch vectors aligned along $\boldsymbol{a}$, $\boldsymbol{b}$, respectively, where $\boldsymbol{a}, \boldsymbol{b} \in [\pm\sigma_x, \pm\sigma_y, \pm\sigma_z]$ (see Fig. 5.3.3). Experimentally, this is done by means of suitably adjusted qubit analyzers, and by counting the number $C(\boldsymbol{a}, \boldsymbol{b})$ of detected photon pairs. From two such spin-measurements, we calculate the normalized *joint-detection probability*

$$P(\boldsymbol{a}, \boldsymbol{b}) = \frac{C(\boldsymbol{a}, \boldsymbol{b})}{C(\boldsymbol{a}, \boldsymbol{b}) + C(\boldsymbol{a}, -\boldsymbol{b})} \qquad (2)$$

The measurement and the results with the fibre delay line, as well as the memory, are detailed in Fig. 5.3.3 and the Supplementary Information. From this data, we re-

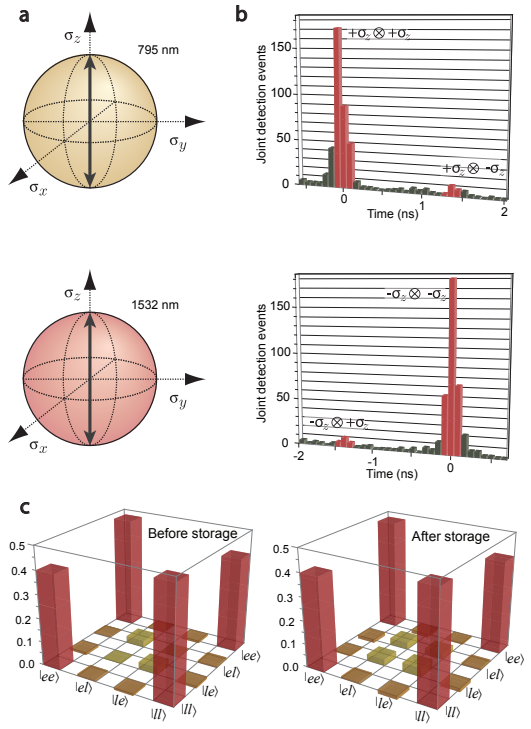


FIG. 5.3.3. **Measurement of density matrices: a**. Visualization of projection measurements. The measurement settings for the 795-nm (or 1,532-nm) qubit analyser are depicted on the upper (or lower) Bloch sphere. The example shows joint settings that enable calculating normalized probabilities for projections onto $\sigma_z \otimes \sigma_z$ $\sigma_z \otimes -\sigma_z$. **b**. Results for joint projection measurement after storage. The top (bottom) histogram displays joint detection events for the projection onto $\sigma_z \otimes \sigma_z$ and $\sigma_z \otimes -\sigma_z$($-\sigma_z \otimes \sigma_z$ and $-\sigma_z \otimes -\sigma_z$) as a function of the time difference between detections of the 795-nm and the 1,532-nm photons. The desired events are those within the red-highlighted time windows. This allows us to calculate the joint-detection probabilities for projections onto $\sigma_z \otimes \sigma_z$ and $\sigma_z \otimes -\sigma_z$ (for results with other joint settings see the Supplementary Information). **c**. Density matrices. Density matrices were calculated using a maximum-likelihood estimation for the bi-photon states before and after storage. Only the real parts are shown-the absolute values of all imaginary components are below 0.04.

construct the bi-photon states before and after storage in terms of their density matrices ρ_{in} and ρ_{out}, depicted in Fig. 5.3.3, using a maximum likelihood estimation [27]. This, in turn, allows us to examine the entanglement of formation [28], a measure that indicates entanglement if it exceeds zero; it is upper-bounded by one. The results, listed in Table 5.3.1, clearly show the presence of entanglement in ρ_{in} and ρ_{out} and, within experimental uncertainty, establish that the storage process preserves entanglement without measurable degradation. Furthermore, we note that the fidelity $\mathcal{F}$ between ρ_{in} and ρ_{out} is close to one, and hence the unitary transformation introduced by the storage process is almost the identity transformation.

In addition, as a second entanglement measure, we perform tests of the Clauser–Horne–Shimony–Holt (CHSH) Bell inequality [6]. This test indicates non-local correlations and thus the possibility of using the bi-photons for entanglement-based quantum key distribution [8] if the sum:

$$S = |E(\boldsymbol{a},\boldsymbol{b}) + E(\boldsymbol{a'},\boldsymbol{b}) + E(\boldsymbol{a},\boldsymbol{b'}) - E(\boldsymbol{a'},\boldsymbol{b'})| \quad (3)$$

of four correlation coefficients

$$E(\boldsymbol{a},\boldsymbol{b}) = \frac{C(\boldsymbol{a},\boldsymbol{b}) - C(\boldsymbol{a},-\boldsymbol{b}) - C(-\boldsymbol{a},\boldsymbol{b}) + C(-\boldsymbol{a},-\boldsymbol{b})}{C(\boldsymbol{a},\boldsymbol{b}) + C(\boldsymbol{a},-\boldsymbol{b}) + C(-\boldsymbol{a},\boldsymbol{b}) + C(-\boldsymbol{a},-\boldsymbol{b})} \quad (4)$$

with appropriately chosen settings $\boldsymbol{a}$, $\boldsymbol{a'}$ and $\boldsymbol{b}$, $\boldsymbol{b'}$ exceeds the classical bound of two; quantum mechanically it is upper-bounded by $2\sqrt{2}$. As detailed in Table 5.3.1, we find $S_{in} = 2.379 \pm 0.034 > 2$ before the memory and, crucially, $S_{out} = 2.25 \pm 0.06 > 2$, which is in agreement with the value $S_{th} = 2.2 \pm 0.22$ predicted from the reconstructed density matrix ρ_{out}. This validates the suitability of our set-up for quantum communication.

Our investigation provides an example of entanglement being transferred between physical systems of different nature, thereby adding evidence that this fundamental quantum property is not as fragile as is often believed. Furthermore, our broadband integrated approach permits the linkage of a promising quantum storage device with extensively used, high-performance sources of photons in bi- and multi-partite entangled states [6]. Although the storage efficiency and the storage time need to be significantly increased, and the moment of recall was pre-set, this study opens the way to new investigations of fundamental and applied aspects of quantum physics. Having increased the storage bandwidth also significantly facilitates the building of future quantum networks, because mutual frequency matching of photons and distant quantum memories will be simple. In addition, a large storage bandwidth –that is, the possibility to encode quantum information into short optical pulses– allows us to increase the number of temporal modes that can be stored during a given time. This enhances the flow of quantum information through a network and decreases the time needed to establish entanglement over a large distance using a quantum repeater [1,2].

We note that, parallel to this work, Clausen et al. have demonstrated the storage of an entangled photon using a neodymium-doped crystal [29].

Acknowledgment

This work is supported by NSERC, QuantumWorks, General Dynamics Canada, iCORE (now part of Alberta Innovates), CFI, AAET and FQRNT. We thank C. La

	Entanglement of formation (%)	Purity (%)	Fidelity with $\|\phi^+\rangle$	Input/output fidelity (%)	Expected S_{th}	Measured S
ρ_{in}	64.4 ±4.2	75.7 ± 2.4	86.2±1.5		2.235 ±0.085	2.379 ±0.034
ρ_{out}	65 ±11	76.3±5.9	86.6 ±3.9	95.4 ±2.9	2.2 ±0.22	2.25 ±0.060

TABLE 5.3.1. **Entanglement measures, purities and fidelities:** Entanglement of formation (normalized with respect to the entanglement of formation of $|\phi^+\rangle$, purity P=tr(ρ^2)), fidelity with $|\phi^+\rangle$, input–output fidelity $\mathcal{F} = \left(\mathrm{tr}\sqrt{\sqrt{\rho_{out}}\rho_{in}\sqrt{\rho_{out}}}\right)^2$ (referring to the fidelity of ρ_{out} with respect to ρ_{in}), and expected and experimentally obtained S values for tests of the CHSH Bell inequality (measured for $\boldsymbol{a} = \sigma_x$, $\boldsymbol{a'} = \sigma_y$, $\boldsymbol{b} = \sigma_x + \sigma_y$ and $\boldsymbol{b'} = \sigma_x - \sigma_y$). The correlation coefficients used to compute S and the calculation of S_{th} are detailed in the Supplementary Information. We note that the original state (and hence the recalled state) has limited purity and fidelity with $|\phi^+\rangle$. This is due to the probabilistic nature of our spontaneous parametric down-conversion source, which features a non-negligible probability of generating more than two photons simultaneously [26]. Uncertainties indicate one-sigma standard deviations and are estimated from Poissonian detection statistics and using a Monte Carlo simulation

Mela, T. Chanelière, T. Stuart, V. Kiselyov and C. Dascollas for help during various stages of the experiment, C. Simon, K. Rupavatharam and N. Gisin for discussions, and A. Lvovsky for lending us a single-photon detector.

* Current address: Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, 1211 Geneva, Switzerland

[1] Lvovsky, A. I., Sanders, B. C., &. Tittel, W. Optical quantum memory. Nature Photon. 3, 706–714 (2009).

[2] Sangouard, N., Simon, C., de Riedmatten, H. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. Preprint at http://arxiv.org/abs/ 0906.2699 (2009).

[3] Kimble, H. J. The quantum Internet. Nature 453, 1023–1030 (2008).

[4] de Riedmatten, H., Afzelius, M., Staudt, M. U., Simon, C. & Gisin, N. A solid–state light–matter interface at the single-photon level. Nature 456, 773–777 (2008).

[5] Usmani, I., Afzelius, M., de Riedmatten, H. & Gisin, N. Mapping multiple photonic qubits into and out of one solid–state atomic ensemble. Nature Commun. 1, 1–7 (2010).

[6] Pan, J.-W., Chen, Z.-B., Zukowski, M., Weinfurter, H. & Zeilinger, A. Multi-photon entanglement and interferometry. Preprint at http://arxiv.org/abs/0805.2853 (2008).

[7] Sohler, W. et al. Integrated optical devices in lithium niobate. Opt. Photon. News 24–31 (January 2008).

[8] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. Rev. Mod. Phys. 74, 145–195 (2002).

[9] Julsgaard, B., Sherson, J. & Cirac, J. I. J. Fiurasek, J. & Polzik, E. S. Experimental demonstration of quantum memory for light. Nature 432, 482–486 (2004).

[10] Chanelière, T. et al. Storage and retrieval of single photons transmitted between remote quantum memories. Nature 438, 833–836 (2005).

[11] Eisaman, M. D. et al. Electromagnetically induced transparency with tunable single-photon pulses. Nature 438, 837–841 (2005).

[12] Honda, K. et al. Storage and retrieval of a squeezed vacuum. Phys. Rev. Lett. 100, 093601 (2008).

[13] Appel, J., Figueroa, E., Korystov, D., Lobino, M. & Lvovsky, A. Quantum memory for squeezed light. Phys. Rev. Lett. 100, 093602 (2008).

[14] Hedges, M. P., Longdell, J. J., Li, Y. & Sellars, M. J. Efficient quantum memory for light. Nature 465, 1052–1056 (2010).

[15] Boozer, A. D. et al. Reversible state transfer between light and a single trapped atom. Phys. Rev. Lett. 98, 193601 (2007).

[16] Choi, C. S. Deng, H. Laurat, J. & Kimble, H. J. Mapping photonic entanglement into and out of a quantum memory. Nature 452, 67–71 (2008).

[17] Akiba, K., Kashiwagi, K. Arikawa, M. & Kozuma, M. Storage and retrieval of nonclassical photon pairs and conditional single photons generated by the parametric down-conversion process. N. J. Phys. 11, 013049 (2009).

[18] Jin, X.-M. et al. Quantum interface between frequency-uncorrelated down converted entanglement and atomic-ensemble quantum memory. Preprint at http://arxiv.org/abs/1004.4691 (2011).

[19] Chou, C. W. et al. Measurement-induced entanglement for excitation stored in remote atomic ensembles. Nature 438, 828–832 (2005).

[20] Matsukevich, D. N. et al. Entanglement of a photon and a collective atomic excitation. Phys. Rev. Lett. 95, 040405 (2005).

[21] Yuan, Z.-S. et al. Experimental demonstration of a BDCZ quantum repeater node. Nature 454, 1098–1101 (2008).

[22] Blinov, B. B., Moehring, D. L., Duan, L.M. & Monroe, C. Observation of entanglement between a single trapped atom and a single photon. Nature 428, 153–157 (2004).

[23] Togan, E. et al. Quantum entanglement between an optical photon and a solid state spin qubit. Nature 466, 730–734 (2010).

[24] Longdell, J., Fraval, E., Sellars, M. & Manson, N. Stopped light with storage times greater than one second using electromagnetically induced transparency in a solid. Phys. Rev. Lett. 95, 063601 (2005).

[25] Marcikic, I. et al. Time-bin entangled qubits for quantum communication created by femtosecond pulses. Phys. Rev. A 66, 062308 (2002).

[26] Sinclair, N. et al. Spectroscopic investigations of a Ti:Tm:$LiNbO_3$ waveguide for photon-echo quantum memory. J. Lumin. 130, 1586–1593 (2010).

[27] Altepeter, J. B., Jeffrey, E. R., &. Kwiat, P. G. Photonic state tomography. Adv. At. Mol. Opt. Phys. 52, 105–159 (2005).

[28] Plenio, M. B. & Virmani, S. An introduction to entanglement measures. Quant. Inf. Comput. 7, 1–51 (2007).

[29] Clausen, C. et al. Quantum storage of photonic entanglement in a crystal. Nature doi:10.1038/nature09662.

Chapter 6

Outlook and Summary

EPR quickly realized that the surprising correlations between measurement results on entangled particles were at odds with the widely held beliefs of locality and realism. However, it took another thirty years before Bell was able to mathematically prove that the correlations allowed by quantum mechanics were impossible to explain by local hidden variables. Twenty years later, applications based on quantum correlations began to appear. Among those applications is QKD, which enables secure transmission of cryptographic keys. Today, fundamental tests of quantum mechanics continue through continued violations of Bell inequalities in increasingly exotic situations. Most believe that a loophole free Bell test with photons will be performed soon. Commercial QKD systems have already been released and are used over short distances within cities. Research groups continue to develop new systems with higher key-rates over longer distances and with less vulnerabilities to side-channel attacks. Researchers are also working to achieve quantum communication over more than a few hundred kilometres, which requires the development of new technologies to circumvent exponential loss with distance. Quantum repeaters, involving entangled photon pairs, entangling measurements over long-distances as well as quantum memories, are one solution being actively researched. Quantum repeaters may one day allow for world-wide quantum communication, including quantum cryptography and fundamental tests of quantum mechanics.

The main goal of this thesis was to study quantum entanglement from a novel fundamental perspective and harness its correlations for applications in quantum communication. Towards this goal, we have built and characterized a high-fidelity source of entanglement and used it for a variety of tests of quantum mechanics. This has included Bell inequalities, a Leggett inequality as well as a general bound on the predictive power about measure-

ment results on members of entangled qubits, with which one can rule out general non-local alternative theories. Our hope is that this work will continue and lead to higher-fidelity entanglement sources and experiments that close loopholes.

In terms of applications of quantum entanglement, we have studied a new protocol for quantum cryptography, MDI-QKD, that uses entangling measurements to remove all detector-based side-channel attacks. We developed a detailed model of the protocol, confirmed its validity by comparing its predictions to measurements with our MDI-QKD system, and then used it to optimize parameters to maximize secret key rates. We then deployed our system across the city of Calgary and demonstrated the feasibility of both real-world MDI-QKD and Bell-state measurements. The results of these studies suggest several directions for near future research activities. We are working towards an automated system that produces higher secret key rates with more stringent security bounds. Automating the system requires integration with the QC2 Cryptography team's hardware to facilitate random state selection and necessary post processing as well as further development of the control systems that maintain indistinguishability, such as an automatic laser-frequency adjustment system operating with high-stability lasers. To achieve higher key rates we are also pursuing integrating the system with high-efficiency, low-noise SSPDs (discussed in Chapter 4), and changing the existing state generation hardware to allow projection measurements onto multiple Bell states. Finally, we believe that with further upgrades (such as higher extinction intensity modulators) we can close state preparation side channels arising from imperfectly prepared states. These, mostly technological upgrades, will move our existing experiments towards a fully developed, real-world system.

In moving towards long-distance applications we have demonstrated a number of important steps towards a functioning quantum repeater. By interfacing a source of entangled photon pairs with our quantum memories we demonstrated high-fidelity quantum state storage and that quantum entanglement is preserved during storage. In addition, by performing

two-photon interference experiments and Bell-state measurements, we demonstrated that the memories preserve the photonic wave function in all degrees of freedom. We are now preparing to perform further proof-of-principle experiments towards implementing a quantum repeater. These involve using current entanglement sources to entangle two quantum memories via entanglement swapping. Afterwards, we plan to develop frequency multi-mode sources of entangled photon pairs suitable for storage in our quantum memories. Such sources could be used to generate heralded entangled photon pairs and also to implement quantum repeater architectures based on multi-mode storage and mode shuffling. Our longer term goal is to demonstrate an elementary link of a quantum repeater and in the future, use quantum repeaters to out perform the direction transmission of entanglement.

This thesis has focused on fundamental tests and applications with quantum entanglement. We have demonstrated the usefulness of new technologies for quantum communication in general. Overall, this thesis has contributed to the merging of once-independent experimental research directions towards a collective goal. Specifically, work on entangled photon pair sources and work on quantum memories was combined and to allow for the storage of entangled photons. In addition, the MDI-QKD protocol required implementing a real-world BSM, which is also needed in quantum repeaters. For the future, it is clear how to advance individual directions while at the same time developing tools that are compatible with, and can be directly implemented in, quantum repeater architectures.

The important achievements for next-generation quantum cryptography systems and future quantum repeaters has advanced the field towards future quantum communications and, I hope, inspired additional efforts. The quantum world may be a strange one, but it is destined to become an ever increasing part of our communication infrastructure.

Bibliography

[1] A. Einstein, B. Podolsky, N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777, 1935.

[2] E. Schrödingier. Die gegenwüarise Situation in der Quantenmechanik (the present situation in quantum mechanics). *Naturwissenschaften*, 23:807, 1935.

[3] J. S. Bell. On the Einstein-Poldolsky-Rosen paradox. *Physics*, 1:195, 1964.

[4] C. H. Bennett, G. Brassard. Quantum Cryptography: Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, page 175, 1984.

[5] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:66, 1991.

[6] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden. Quantum Cryptography. *Rev. Mod. Phys.*, 74:145, 2002.

[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, M. Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301, 2009.

[8] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. K. Wootters. Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels. *Phys. Rev. Lett.*, 70:1985, 1993.

[9] M. Zukowski, A. Zeilinger, M. A. Horne, A. K. Ekert. "event-ready-detectors" bell experiment via entanglement swapping. *Phys. Rev. Lett.*, 71:4287, 1993.

[10] C. H. Bennett, D. P. DiVincenzo. Quantum information and computation. *Nature*, 404:247, 2000.

[11] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, G. J. Milburn. Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.*, 79:135, 2007.

[12] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880, 1969.

[13] S. J. Freedman, J. F. Clauser. Experimental Test of Local Hidden-Variable Theories. *Phys. Rev. Lett.*, 28:938, 1972.

[14] G. Roger A. Aspect, P. Grangier. Experimental tests of realistic local theories via bell's theorem. *Phys. Rev. Lett.*, 47:460, 1981.

[15] A. Aspect, P. Grangier, G. Roger. Experimental Realization of Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment*: A New Violation of Bell's Inequalities. *Phys. Rev. Lett.*, 49:91, 1982.

[16] A. Aspect, J. Dalibard, G. Roger. Experimental Test of Bell's Inequalities Using Time-Varying Analyzers. *Phys. Rev. Lett.*, 49:1804, 1982.

[17] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, Y. Shih. New High-Intensity Source of Polarization-Entangled Photon Pairs. *Phys. Rev. Lett.*, 75:4337, 1995.

[18] W. Tittel, J. Brendel, H. Zbinden, N. Gisin. Violation of Bell Inequalities by Photons More Than 10 km Apart. *Phys. Rev. Lett.*, 81:3563, 1998.

[19] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, A. Zeilinger. Violation of Bell's Inequality under Strict Einstein Locality Conditions. *Phys. Rev. Lett.*, 81:5039, 1998.

[20] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, D. J. Wineland. Experimental violation of a Bell's inequality with efficient detection. *Nature*, 409:791, 2001.

[21] R. Ursin, F. Tiefenbacher, T. Shmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trokek, B. Omer, M. Furst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, A. Zeilinger. Entanglement-based quantum communication over 144 km. *Nature Physics*, 3:481, 2007.

[22] T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. Langford, T. Jennewein, A. Zeilinger. Violation of local realism with freedom of choice. *Proceedings of the National Academy of Sciences USA*, 107:19708, 2010.

[23] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, A. Zeilinger. Bell violation using entangled photons without the fair-sampling assumption. *Nature advance online publication*, 2013.

[24] P. H. Eberhard. Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment. *Phys. Rev. A*, 47:747, 1993.

[25] M. Arndt, O. Nairz, J. Vos-Andreae, C. Keller, G. van der Zouw, A. Zeilinger. Wave-particle duality of C_{60} molecules. *Nature*, 401:680, 1999.

[26] M. Aspelmeyer, T. J. Kippenberg, F. Marquardt. Cavity Optomechanics. *arXiv:1303.0733*, 2013.

[27] A. J. Leggett. Nonlocal hidden-variable theories and quantum mechanics: An incompatibility theorem. *Foundations of Physics*, 33:1469, 2003.

[28] S. Gröblacher, T. Paterek, R. Kaltenbaek, C. Brukner, M. Zukowski, M. Aspelmeyer, A. Zeilinger. An experimental test of non-local realism. *Nature*, 446:871, 2007.

[29] C. Branciard, A. Ling, N. Gisin, C. Kurtsiefer, A. Lamas-Linares, V. Scarani. Experimental Falsification of Leggett's Nonlocal Variable Model. *Phys. Rev. Lett.*, 99:210407, 2007.

[30] http://www.idquantique.com, http://www.magiqtech.com.

[31] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, S. Ten. High rate long-distance quantum key distribution over 250 km of ultra low loss fibres. *New Journal of Physics*, 11:075003, 2009.

[32] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, Th. Scheidl, J. Perdigues, Z. Sodnik, J. G. Rarity, A. Zeilinger, H. Weinfurter. Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. *Phys. Rev. Lett.*, 98:010504, 2007.

[33] M. Peev *et al.* The SECOQC quantum key distribution network in Vienna. *New Journal of Physics*, 11:075001, 2009.

[34] M. Sasaki *et al.* Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Exp.*, 19:10387, 2011.

[35] D. Pearson. High-Speed QKD Reconciliation using Forward Error Correction. *Quantum Communication, Measurement and Computing. AIP Conference Proceedings*, 734:299, 2004.

[36] C. H. Bennett, G. Brassard, C. Crépeau, U. M. Maurer. Generalized Privacy Amplification. *IEEE Transactions on Information Theory*, 41:6, 1995.

[37] C. H. Bennett, G. Brassard, N. D. Mermin. Quantum Cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557, 1992.

[38] W. K. Wootters, W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802, 1982.

[39] G. Brassard, N. Lütkenhaus, T. Mor, B. C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85:1330, 2000.

[40] S. Nauerth, M. Fŕust, T. Schmitt-Manderbach, H. Weier, H. Weinfurter. Information leakage via side channels in freespace BB84 quantum cryptography. *New Journal of Physics*, 11:065001, 2009.

[41] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4:686, 2010.

[42] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, H.-K. Lo. Quantum Hacking: Experimental demonstration of time-shift attack against practical quantum key distribution systems. *Phys. Rev. A*, 78:042333, 2008.

[43] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, G. Ribordy. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A*, 73:022320, 2006.

[44] W. Hwang. Quantum key distribution with high loss: Towards global secure communication. *Phys. Rev. Lett.*, 91:057901, 2003.

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

[46] H.-K. Lo, X. Ma, K. Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, 2005.

[47] H.-K. Lo, M. Curty and B. Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, 2012.

[48] S. L. Braunstein, S. Pirandola. Side-channel-free quantum key distribution. *Phys. Rev. Lett.*, 108:130502, 2012.

[49] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani. Device-Independent Security of Quantum Cryptography against Collective Attacks. *Phys. Rev. Lett.*, 98:230501, 2007.

[50] L. Masanes, S. Pironio, A. Acín. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Comm.*, 2:238, 2011.

[51] C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner, N. Gisin. Device-independent quantum key distribution with local Bell test. *arXiv:1208.0023 [quant-ph]*, 2012.

[52] R. Ursin, T. Jennewein, J. Kofler, J. M. Perdigues, L. Cacciapuoti, C. J. de Matos, M. Aspelmeyer, A. Valencia, T. Scheidl, A. Fedrizzi, A. Acin, C. Barbieri, G. Bianco, C. Brukner, J. Capmany, S. Cova, D. Giggenbach, W. Leeb, R. H. Hadfield, R. Laflamme, N. Lutkenhaus, G. Milburn, M. Peev, T. Ralph, J. Rarity, R. Renner, E. Samain, N. Solomos, W. Tittel, J. P. Torres, M. Toyoshima, A. Ortigosa-Blanch, V. Pruneri, P. Villoresi, I. Walmsley, G. Weihs, H. Weinfurter, M. Zukowski, A. Zeilinger. Space-QUEST: Experiments with quantum entanglement in space. *59th International Astronautical Congress (IAC)*, A2.1.3, 2008.

[53] H.-J. Briegel, W. Dür, J. I. Cirac, P. Zoller. Quantum Repeaters: the Role of Imperfect Local Operations in Quantum Communication. *Phys. Rev. Lett.*, 81:5932, 1998.

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

[55] A. I. Lvovsky, B. C. Sanders, W. Tittel. Optical quantum memory. *Nature Photonics*, 3:706, 2009.

[56] C. Simon, M. Afzelius, J. Appel, A. Boyer de la Giroday, S. J. Dewhurst, N. Gisin, C. Y. Hu, F. Jelezko, S. Krpll, J. H. Müller, J. Nunn, E. S. Polzik, J. G. Rarity, H. De Riedmatten, W. Rosenfeld, A. J. Shields, N. and Sköld, R. M. Stevenson, R. Thew, I. A. Walmsley, M. C. Weber, H. Weinfurter, J. Wrachtrup, R. J. Young. Quantum memories. A review based on the European integrated project. *The European Physical Journal D* , 58:1, 2010.

[57] W. Tittel, M. Afzelius, T. Chanelière, R. L. Cone, S. Kröll, S. A. Moiseev, M. Sellars. Photon-echo quantum memory in solid state systems. *Laser & Photonics Reviews*, 4(2):244, 2010.

[58] C. Simon, H. de Riedmatten, M. Afzeilus, N. Sangouard, H. Zbinden, N. Gisin. Quantum repeaters with photon pair sources and multimode memories. *Phys. Rev. Lett.*, 98(190503), 2007.

[59] L. Duan, M. D. Lukin, J. I. Cirac, P. Zoller. Long-distance quantum communication with atomic ensembles and linear optics . *Nature*, 414:413, 2001.

[60] w. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, K. Nemoto. From quantum multiplexing to high-performance quantum networking. *Nature Photonics*, 4(792), 2010.

[61] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, P. H. Eberhard. Ultrabright source of polarization-entangled photons. *Phys. Rev. A*, 60:R773, 1999.

[62] W. Tittel, G. Weihs. Photonic Entanglement for Fundamental Tests and Quantum Communication. *Quantum Information and Computation*, 1:3, 2001.

[63] J. Brendel, N. Gisin, W. Tittel, H. Zbinden. Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication. *Phys. Rev. Lett.*, 82:2594, 1999.

[64] C. K. Hong, Z. Y. Ou, L. Mandel. Measurement of Subpicosecond Time Intervals Between Two Photons by Interference. *Phys. Rev. Lett.*, 59:2044, 1987.

[65] N. Lütkenhaus, J. Calsamiglia, K. A. Suominen. Bell measurements for teleportation. *Phys. Rev. A*, 59:3295, 1999.

[66] T. E. Stuart, J. A. Slater, R. Colbeck, R. Renner, W. Tittel. Experimental Bound on the Maximum Predictive Power of Physical Theories. *Phys. Rev. Lett.*, 109:020402, 2012.

[67] D. Bohm. A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. I. *Phys. Rev.*, 85:166, 1952.

[68] R. Colbeck, R. Renner. No extension of quantum theory can have improved predictive power. *Nature Comm.*, 2:511, 2011.

[69] T. M. Cover, J. A. Thomas. Elements of Information Theory. *John Wiley and Sons Inc.*, 2nd, 2006.

[70] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. P. Temporo, J. P. von der Weid. Proof-of-principle demonstration of measurement device independent QKD using polarization qubits. *arXiv:1207.6345 [quant-ph]*, 2012.

[71] 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, Q. Zhang, J.-W. Pan. Experimental measurement-device-independent quantum key distribution. *arXiv:1209.6178 [quant-ph]*, 2012.

Appendix A

Supplemental Materials and Supplementary Information

This appendix is composed of supplemental materials and supplemental information from the following articles:

3.2 T. E. Stuart, J. A. Slater, R. Colbeck, R. Renner and W. Tittel, An experimental test of all theories with predictive power beyond quantum theory, *Physical Review Letters* **109** (2): 020402, 9 July 2012.

4.2 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, arXiv.org:1304.2463, 9 April 2013.

5.2 J. Jin, J. A. Slater, E. Saglamyurek, N. 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, arXiv.org:1302.2177, 8 February 2013.

5.3 E. Saglamyurek, N. Sinclair, J. Jin, J. A. Slater, D. Oblak, F. Bussières, M. George, R. Ricken, W. Sohler and W. Tittel, Broadband waveguide quantum memory for entangled photons, *Nature* **469** (7331): 512 - 515, 12 January 2011.

Supplemental Material: An experimental bound on the maximum predictive power of physical theories

Terence E. Stuart,[1] Joshua A. Slater,[1] Roger Colbeck,[2,3] Renato Renner,[2] and Wolfgang Tittel[1]

[1]*Institute for Quantum Information Science, and Department of Physics and Astronomy, University of Calgary, 2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada.*
[2]*Institute for Theoretical Physics, ETH Zurich, Wolfgang-Pauli-Str. 27, 8093 Zurich, Switzerland.*
[3]*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario N2L 2Y5, Canada.*

I. PROOF OF THE BOUND

In this section, we prove the bound given in Equation (1) in the main text, which is stated as Lemma 1 below. We use a bipartite scenario in which two spacelike separated measurements are performed on a maximally entangled state. We denote the choices of observable $A \in \{0, 2, \ldots, 2N-2\}$ and $B \in \{1, 3, \ldots, 2N-1\}$ and their outcomes $X \in \{+1, -1\}$ and $Y \in \{+1, -1\}$, respectively[1]. We additionally consider information that might be provided by an alternative theory (denoted Ξ), which is modelled as an additional system with input C and output Z [1]. We assume that this information is static, in the sense that its behaviour is independent of the coordinates associated with C and Z. If one makes the assumption that the measurements can be chosen freely, then the joint distribution $P_{XYZ|ABC}$ satisfies the non-signalling conditions

$$P_{XY|ABC} = P_{XY|AB} \tag{1}$$
$$P_{XZ|ABC} = P_{XZ|AC} \tag{2}$$
$$P_{YZ|ABC} = P_{YZ|BC}. \tag{3}$$

A proof of this was given in [1], which we now recap for completeness.

Recall that the free choice assumption states that for a parameter, A, to be free, it must be uncorrelated with all variables outside its future lightcone[2]. The setup is such that the measurements specified by A and B are spacelike separated and, since Ξ is static, we can consider its observation to also be spacelike separated from the other measurements.

We assume A is a free choice, which corresponds mathematically to the condition

$$P_{A|BCYZ} = P_A. \tag{4}$$

Furthermore, using the definition of conditional probability ($P_{Q|R} := P_{QR}/P_R$), we can write

$$P_{YZA|BC} = P_{YZ|BC} \times P_{A|BCYZ} = P_A \times P_{YZ|BC} \ ,$$

where we inserted (4) to obtain the second equality. Similarly, we have

$$P_{YZA|BC} = P_{A|BC} \times P_{YZ|ABC} = P_A \times P_{YZ|ABC} \ .$$

Comparing these two expressions for $P_{YZA|BC}$ yields the non-signalling condition (3). Repeating this argument symmetrically, the other non-signalling conditions can be similarly inferred.

Note that standard proofs of Bell's theorem and related results assume both no-signalling and that measurements are chosen freely (see, for example, [3] for a statement of Bell's notion of free choice, which is the same as ours). Although free choice implies no-signalling, the converse does not hold. Instead, no-signalling is needed for free choices to be possible, but does not imply that they are actually made.

---

[1] Note that the measurements we speak of in the Supplemental Material have a slightly different form than those in the main text. Specifically, we now assume that measurements behave ideally, projecting onto one of two basis elements and leading to one of the two outcomes ± 1. In a real experiment, there is always the additional possibility of no photon detection (let us denote this outcome 0). The measurements discussed in the main text are configured to distinguish $+1$ from either -1 or 0, or to distinguish -1 from either $+1$ or 0. Both of these measurements are used in the experiment to infer the distribution of the ideal measurement with outcomes ± 1.

[2] Note that this requirement can be seen as a prerequisite for non-contextuality, as pointed out in [2], where an alternative proof that quantum theory cannot be extended, based on the assumption of non-contextuality, is offered.

Lemma 1 gives a bound on the increase in predictive power of any alternative theory in terms of the strength of correlations and the bias of the individual outcomes. The bound is expressed in terms of the variational distance $D(P_W, Q_W) := \frac{1}{2}\sum_w |P_W(w) - Q_W(w)|$, which has the following operational interpretation: if two distributions have variational distance at most δ, then the probability that we ever notice a difference between them is at most δ.

The bias is quantified by[3] $\nu_N := \max_a D(P_{X|a}, P_{\bar{X}})$, where $P_{\bar{X}}$ is the uniform distribution on X. To quantify the correlation strength, we define

$$I_N := P(X = Y|A = 0, B = 2N-1) \; + \sum_{\substack{a,b \\ |a-b|=1}} P(X \neq Y|A = a, B = b) \; . \tag{5}$$

This is equivalent to Equation (6) in the main text. We remark that $I_N \geq 1$ is a Bell inequality, i.e. is satisfied by any local hidden variable model.

Lemma 1. *For any non-signalling probability distribution, $P_{XYZ|ABC}$, we have*

$$D(P_{Z|abcx}, P_{Z|abc}) \leq \delta_N := \frac{I_N}{2} + \nu_N \tag{6}$$

for all a, b, c, and x.

To connect this back to the main text, we remark that the Markov chain condition $X \leftrightarrow A \leftrightarrow \Xi$ is equivalent to $P_{Z|abcx} = P_{Z|abc}$ (which corresponds to Ξ not being of use to predict X). Hence, from the operational meaning of the variational distance (given above), (6) can be interpreted that X and Z can be treated as uncorrelated, except with probability at most δ_N.

The proof is an extension of an argument given in [1] which is based on *chained Bell inequalities* [4–6] and generalizes results of [7–9]. Many steps of this proof mirror those in [1], which we repeat here for completeness. However, note that the bound derived in this Lemma is tighter than that of [1].

Proof. We first consider the quantity I_N evaluated for the conditional distribution $P_{XY|AB,cz} = P_{XY|ABCZ}(\cdot,\cdot|\cdot,\cdot,c,z)$, for any fixed c and z. The idea is to use this quantity to bound the variational distance between the conditional distribution $P_{X|acz}$ and its negation, $1 - P_{X|acz}$, which corresponds to the distribution of X if its values are interchanged. If this distance is small, it follows that the distribution $P_{X|acz}$ is roughly uniform.

For $a_0 := 0$, $b_0 := 2N-1$, we have

$$\begin{aligned}
I_N(P_{XY|AB,cz}) &= P(X = Y|A = a_0, B = b_0, C = c, Z = z) + \sum_{\substack{a,b \\ |a-b|=1}} P(X \neq Y|A = a, B = b, C = c, Z = z) \\
&\geq D(1 - P_{X|a_0b_0cz}, P_{Y|a_0b_0cz}) + \sum_{\substack{a,b \\ |a-b|=1}} D(P_{X|abcz}, P_{Y|abcz}) \\
&= D(1 - P_{X|a_0cz}, P_{Y|b_0cz}) + \sum_{\substack{a,b \\ |a-b|=1}} D(P_{X|acz}, P_{Y|bcz}) \\
&\geq D(1 - P_{X|a_0cz}, P_{X|a_0cz}) \\
&= 2D(P_{X|a_0b_0cz}, P_{\bar{X}}) \; .
\end{aligned} \tag{7}$$

The first inequality follows from the fact that $D(P_{X|\Omega}, P_{Y|\Omega}) \leq P(X \neq Y|\Omega)$ for any event Ω (a short proof of this can be found in [9]). Furthermore, we have used the non-signalling conditions $P_{X|abcz} = P_{X|acz}$ (from (2)) and $P_{Y|abcz} = P_{Y|bcz}$ (from (3)), and the triangle inequality for D. By symmetry, this relation holds for all a and b. We hence obtain $D(P_{X|abcz}, P_{\bar{X}}) \leq \frac{1}{2} I_N(P_{XY|AB,cz})$ for all a, b, c and z.

---

[3] A note on notation: we usually use lower case to denote particular instances of upper case random variables.

We now take the average over z on both sides of (7). First, the left hand side gives

$$\begin{aligned}\sum_z P_{Z|abc}(z) I_N(P_{XY|AB,cz}) &= \sum_z P_{Z|c}(z) I_N(P_{XY|AB,cz}) \\ &= \sum_z P_{Z|a_0b_0c}(z) P(X=Y|a_0,b_0,c,z) + \sum_{\substack{a,b \\ |a-b|=1}} \sum_z P_{Z|abc}(z) P(X\neq Y|a,b,c,z) \\ &= P(X=Y|a_0,b_0,c) + \sum_{\substack{a,b \\ |a-b|=1}} P(X\neq Y|a,b,c) \\ &= I_N(P_{XY|AB,c}) \ , \end{aligned} \tag{8}$$

where we used the non-signalling condition $P_{Z|abc} = P_{Z|c}$ (which is implied by (2) and (3)) several times. Next, taking the average on the right hand side of (7) yields $\sum_z P_{Z|abc}(z) D(P_{X|abcz}, P_{\bar{X}}) = D(P_{XZ|abc}, P_{\bar{X}} \times P_{Z|abc})$, so we have

$$2D(P_{XZ|abc}, P_{\bar{X}} \times P_{Z|abc}) \leq I_N(P_{XY|AB,c}) = I_N(P_{XY|AB}). \tag{9}$$

The last equality follows from the non-signalling condition (1) (if $P(X=Y|a,b,c)$ or $P(X\neq Y|a,b,c)$ depended on c, then there would be signalling from C to A and B).

Furthermore, note that

$$2D(P_{XZ|abc}, P_{\bar{X}} \times P_{Z|abc}) = \sum_z \big|P_{XZ|abc}(-1,z) - \frac{1}{2}P_{Z|abc}(z)\big| + \sum_z \big|P_{XZ|abc}(+1,z) - \frac{1}{2}P_{Z|abc}(z)\big|$$

and that both of the terms on the right hand side are equal (since $P_{Z|abc}(z) = P_{XZ|abc}(-1,z) + P_{XZ|abc}(+1,z)$) i.e. $\sum_z \big|P_{XZ|abc}(x,z) - \frac{1}{2}P_{Z|abc}(z)\big| \leq \frac{I_N}{2}$ for all a, b, c and x. Note also that $D(P_{X|a}, P_{\bar{X}}) = \big|P_{X|a}(x) - \frac{1}{2}\big|$ for all x.

Combining the above, we have

$$\begin{aligned} D(P_{Z|abcx}, P_{Z|abc}) &= \sum_z \big|\frac{1}{2}P_{Z|abcx}(z) - \frac{1}{2}P_{Z|abc}(z)\big| \\ &\leq \sum_z \big|\frac{1}{2}P_{Z|abcx}(z) - P_{X|abc}(x)P_{Z|abcx}(z)\big| + \sum_z \big|P_{X|abc}(x)P_{Z|abcx}(z) - \frac{1}{2}P_{Z|abc}(z)\big| \\ &= \sum_z P_{Z|abcx}(z)\big|\frac{1}{2} - P_{X|abc}(x)\big| + \sum_z \big|P_{XZ|abc}(x,z) - \frac{1}{2}P_{Z|abc}(z)\big| \\ &\leq D(P_{X|a}, P_{\bar{X}}) + \frac{I_N(P_{XY|AB})}{2}. \end{aligned}$$

This establishes the relation (6). □

Tightness

We can also establish that this bound is tight, as follows. Consider a classical model in which, with probability ε, we have $X = Y = Z = -1$, and otherwise $X = Y = Z = +1$ (independently of A, B and C). This distribution has $I_N(P_{XY|AB}) = 1$ and $\nu = \frac{1}{2} - \varepsilon$. It also satisfies $D(P_{Z|abcX=-1}, P_{Z|abc}) = 1 - \varepsilon$, which is equal to the bound implied by (6).

Use of bipartite correlations

The argument leading to the bound in Lemma 1 is based on a bipartite scenario. As mentioned in the main text, measurements on a single system can always be explained by a local hidden variable model. We give a simple argument for this here.

For a single system, we wish to recreate the correlations $P_{X|A}$. To do so, we introduce a hidden variable, Z_a for each possible choice of measurement, $A = a$, distributed according to $P_{Z_a} = P_{X|a}$ (i.e. this hidden variable is distributed exactly as the outcomes of the measurement $A = a$ would be and has the same alphabet). When measurement $A = a$ is chosen, the outcome is given by $X = Z_a$. This local hidden variable model recreates the correlations $P_{X|A}$ precisely. In other words, no experiment on a single system can rule out a local hidden variable model of this type.

Comment on the free choice assumption and the de Broglie-Bohm model

We now discuss our result in light of the de Broglie-Bohm model [10, 11]. There, C is not used, and the parameter Z includes both the wavefuction and the (hidden) particle trajectories that make up that model. Thus, according to the argument we give above, if A can be chosen freely, $P_{YZ|AB} = P_{YZ|B}$ (this is (3) in the case without C), and hence $P_{Y|ABZ} = P_{Y|BZ}$. However, the de Broglie-Bohm model does not, in general, satisfy this relation: the outcome Y is a deterministic function of the wavefunction, the particle positions and *both* A and B. The dependence on A is crucial in order that the model can recreate all quantum correlations. It hence follows that the de Broglie-Bohm model does not satisfy our free choice assumption, and hence it is not in contradiction with our main claim.

II. APPLICATION TO LEGGETT MODELS

In the Leggett model [12], one imagines that improved predictions about the outcomes for measurements on spin-half particles are available. More precisely, each particle has an associated vector (thought of as a hidden direction of its spin) and the outcome distribution is expressed via the inner product with the vector describing the measurement (see Figure 1 in the main text). Denoting the hidden vector for the first particle by $\mathbf{z}$, and its measurement vector $\boldsymbol{\alpha}$ (this is the Bloch vector associated with the chosen measurement direction; it was denoted $\mathbf{S}_A$ ($\mathbf{S}_B$) in the main text), its outcomes are distributed according to

$$P_{X|\boldsymbol{\alpha}\mathbf{z}}(\pm 1) = \frac{1}{2}(1 \pm \boldsymbol{\alpha} \cdot \mathbf{z}). \tag{10}$$

To relate this back to the discussion above, the Leggett model corresponds to the case that there is no C, and where the hidden vectors are contained in Z. Note that Leggett already showed his model to be incompatible with quantum theory [12] and experiments have since falsified it using specific inequalities [13–16]. Here we discuss the model in light of our experiment, which, it turns out, is sufficient to falsify it.

As presented above, the model is not fully specified since the distribution of the hidden vectors, $\mathbf{z}$, is not given. To discuss the implications of our experimental results we refer to four cases (corresponding to different distributions over $\mathbf{z}$). In order to agree with existing experimental observations, the distribution should be such that the uniform distribution is approximately recovered when $\mathbf{z}$ is unknown, i.e. $P_{X|\boldsymbol{\alpha}} = \sum_z P_{\mathbf{Z}}(\mathbf{z}) P_{X|\boldsymbol{\alpha}\mathbf{z}} \cong \frac{1}{2}$.

Before describing the four cases, we first note that adapting our previous analysis (starting from (9), for example) to the case of no C implies

$$\langle D(P_{X|\boldsymbol{\alpha}\mathbf{z}}, P_{\bar{X}}) \rangle_{\mathbf{z}} \leq \delta_N, \tag{11}$$

for all $\boldsymbol{\alpha}$, where $\langle \cdot \rangle_{\mathbf{z}}$ denotes the expectation value over the vectors $\mathbf{z}$. In order to falsify a particular version of the Leggett model, we compute δ_N^{crit}, the smallest increase in predictive power under the assumption that a particular version of the Leggett model is correct (i.e. the smallest value of the left-hand-side of (11) over all $\boldsymbol{\alpha}$). We then show that δ_N^{crit} is above the maximum increase in predictive power compatible with the experimental data, δ_N, hence falsifying that version of Leggett's model.

First Case: We imagine that the vector $\mathbf{z}$ is uniformly distributed between two opposite vectors (i.e. $P_{\mathbf{Z}}(\mathbf{z_0}) = P_{\mathbf{Z}}(\bar{\mathbf{z}}_\mathbf{0}) = \frac{1}{2}$ for some fixed vector $\mathbf{z_0} = -\bar{\mathbf{z}}_\mathbf{0}$) in the same plane on the Bloch sphere as our measurements. From (10), we have $D(P_{X|\boldsymbol{\alpha}\mathbf{z_0}}, P_{\bar{X}}) = D(P_{X|\boldsymbol{\alpha}\bar{\mathbf{z}}_\mathbf{0}}, P_{\bar{X}}) = \frac{|\boldsymbol{\alpha}\cdot\mathbf{z_0}|}{2}$. Hence, from (11) we require $\frac{|\boldsymbol{\alpha}\cdot\mathbf{z_0}|}{2} \leq \delta_N$ for all $\boldsymbol{\alpha}$. In order to make $\max_{\boldsymbol{\alpha}} |\boldsymbol{\alpha} \cdot \mathbf{z_0}|$ as small as possible, i.e. find δ_N^{crit1}, we require the vector $\mathbf{z_0}$ to be as far as possible from any of the possible $\boldsymbol{\alpha}$ vectors. If the fixed vector $\mathbf{z_0}$ is in the plane containing the measurements, this condition leads to $\max_{\boldsymbol{\alpha}} |\boldsymbol{\alpha} \cdot \mathbf{z_0}| = \cos\frac{\pi}{2N}$ (i.e. $\mathbf{z_0}$ is positioned exactly in between two settings for $\boldsymbol{\alpha}$). Hence, this specific version of the Leggett model is falsified if the measured $\delta_N < \delta_N^{\text{crit1}} = \frac{1}{2}\cos\frac{\pi}{2N}$. As shown in Supplemental Table A1.1, this is the case for all values of N assessed.

According to quantum theory, appropriately chosen measurements on a maximally entangled state lead to correlations for which $\delta_N = \frac{N}{2}(1 - \cos\frac{\pi}{2N})$. However, no experimental realization can be noise-free, and this affects the minimum δ_N attainable (see [1, 17]). One way to characterize the imperfection in the experiment is via the visibility. In an experiment with visibility V[4], we instead obtain $\delta_N = \frac{N}{2}(1 - V\cos\frac{\pi}{2N})$, which for fixed V has a minimum at

[4] The visibility is an alternative measure of the quality of the experiment (the fidelity was used in the main text). The visibility can be directly measured, while the fidelity (to the desired state) can be calculated from the state reconstructed tomographically. Assuming isotropic noise as the dominant source of imperfection (i.e. that we actually measure Werner states), fidelity and visibility are related through $V = (4F - 1)/3$.

N	δ_N^{crit1}	δ_N^{crit2}	δ_N^{crit3}	δ_N^{crit4}	δ_N^1	δ_N^2
2	**0.3536**	0.2	0.25	0.1768	0.3131±0.0018	0.3125±0.0025
3	**0.4330**	**0.3062**	**0.25**	0.2165	0.2294±0.0016	0.2437±0.0023
4	**0.4619**	**0.3266**	**0.25**	**0.2310**	0.1904±0.0015	0.2094±0.0023
5	**0.4755**	**0.3362**	**0.25**	**0.2378**	0.1792±0.0014	0.2015±0.0023
6	**0.4830**	**0.3415**	**0.25**	**0.2415**	0.1676±0.0019	0.1942±0.0021
7	**0.4875**	**0.3447**	**0.25**	**0.2437**	0.1644±0.0014	0.1948±0.0021
$V_{\min}$	0.821	0.906	0.946	0.951		

Supplemental Table A1.1: **Leggett models: critical values and experimental data.** This table shows the critical values of δ_N required to rule out each of the four Leggett-type models discussed in the text. Also shown are measured values for δ_N^1 and δ_N^2, where the superscript refers to measurements in the $|H\rangle - |+\rangle$ plane, and the $|+\rangle - |L\rangle$ plane of the Bloch sphere, respectively. Bold values have $\delta_N^1 < \delta_N^{\text{crit } i}$ and, if required $\delta_N^2 < \delta_N^{\text{crit } i}$, i.e. the Leggett model i is ruled out by the data for that N. The values of δ_N^2 are relevant for ruling out the second and fourth model. In the last row of the table, we note the minimum visibility required to rule out each of the four models.

finite N. In the case of this model, the minimum visibility required to falsify it is 0.821 (with such a visibility the model could be ruled out with $N = 3$).

Second case: We now suppose $\mathbf{z}$ is distributed as in the first case, but that $\mathbf{z_0}$ is no longer confined to the plane of measurements. In this case our basic measurements cannot strictly *rule out* this model: in principle, $\mathbf{z_0}$ could be close to orthogonal to the plane containing the measurement vectors. (We remark that if $\mathbf{z_0}$ is completely orthogonal to this plane, then it would not be useful for making predictions.) However, in order to rectify this we can include a second set of measurements in the set of random choices. This set should be identical to the first apart from being contained in an orthogonal plane. We denote the sets $\mathcal{A}_1$ and $\mathcal{A}_2$ and we separately measure the δ_N values for each plane, generating values denoted δ_N^1 and δ_N^2. Analogously to the first case discussed above, this version of the Leggett model is falsified unless for all $\boldsymbol{\alpha} \in \mathcal{A}_1 \cup \mathcal{A}_2$, $|\boldsymbol{\alpha} \cdot \mathbf{z_0}|/2 \leq \min(\delta_N^1, \delta_N^2)$. In order to make $\max_{\boldsymbol{\alpha}} |\boldsymbol{\alpha} \cdot \mathbf{z_0}|$ as small as possible, we require the vectors $\mathbf{z_0}$ to be as far as possible from any of the possible $\boldsymbol{\alpha}$ vectors. Consider now the four vectors $(0, \sin\phi, \cos\phi)$, $(0, -\sin\phi, \cos\phi)$, $(\cos\phi, \sin\phi, 0)$ and $(\cos\phi, -\sin\phi, 0)$ for $\phi \leq \frac{\pi}{4}$ (these represent two neighbouring pairs of measurement vectors (one in each plane), where we have chosen the coordinates such that they are symmetric). The vector equidistant from these (in their convex hull) is $(\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}})$. It is then not possible that for all $\boldsymbol{\alpha} \in \mathcal{A}_1 \cup \mathcal{A}_2$, $|\boldsymbol{\alpha} \cdot \mathbf{z_0}|/2 \leq \min(\delta_N^1, \delta_N^2)$ provided $\max(\delta_N^1, \delta_N^2) < \delta_N^{\text{crit2}} = \frac{1}{2\sqrt{2}} \cos\frac{\pi}{2N}$. As shown in Supplemental Table A1.1, our experiment, which includes measurements of δ_N in an orthogonal plane, also rules out this version of the Leggett model. (The minimum visibility required to rule out this model is 0.906, which could do so using $N = 4$.)

Third case: We consider a slightly modified model in which $\mathbf{z}$ is distributed uniformly over the Bloch sphere. This model is arguably more natural since it is somewhat conspiratorial for $\mathbf{z}$ to be confined to a particular set of orientations with respect to the measurements we perform (particularly if that measurement is chosen freely), and is the model referred to in the main text. In this case, defining θ as the angle between $\boldsymbol{\alpha}$ and $\mathbf{z}$, we compute the left hand side of (11) as

$$\langle D(P_{X|\boldsymbol{\alpha}z}, P_{\bar{X}})\rangle_{\mathbf{z}} = \int_{\theta=0}^{\pi} \mathrm{d}\theta \frac{|\cos\theta| \sin\theta}{4} = \frac{1}{4}.$$

This model is hence excluded if one finds $\delta_N < \delta_N^{\text{crit3}} = \frac{1}{4}$ (measurements are needed only in one plane). As shown in Supplemental Table A1.1, this is the case for $N \geq 3$. (The minimum visibility required to rule out this model is 0.946, which could do so for $N = 5$.)

Fourth case: Here we return to our measurements in two orthogonal planes and ask whether our data is sufficient to falsify the model for any distribution over $\mathbf{z}$. (We can think of this in terms of an adversarial picture. Suppose the set of possible measurement choices is known to an adversary, who can pick the vector $\mathbf{z}$ according to any distribution he likes. The aim is to show that our measurement results are not consistent with any such adversary.) For this model to be correct we need

$$\begin{aligned} \frac{\langle|\boldsymbol{\alpha} \cdot \mathbf{z}|\rangle_{\mathbf{z}}}{2} &\leq \delta_N^1 \text{ for all } \boldsymbol{\alpha} \in \mathcal{A}_1 \\ \frac{\langle|\boldsymbol{\alpha} \cdot \mathbf{z}|\rangle_{\mathbf{z}}}{2} &\leq \delta_N^2 \text{ for all } \boldsymbol{\alpha} \in \mathcal{A}_2. \end{aligned}$$

Again we can parameterize in terms of the four vectors introduced previously. When minimizing with respect to these four, we should take $P_{\mathbf{Z}}$ to have support only on the set $(\sin\theta, 0, \cos\theta)$ (going off this line increases the inner product

with measurement vectors in both sets). We thus have

$$\langle|\boldsymbol{\alpha}\cdot\mathbf{z}|\rangle_{\mathbf{z}} = \begin{cases} \int_\theta \mathrm{d}\theta\rho(\theta)\cos\theta\cos\frac{\pi}{2N} & \text{for all } \boldsymbol{\alpha}\in\mathcal{A}_1 \\ \int_\theta \mathrm{d}\theta\rho(\theta)\sin\theta\cos\frac{\pi}{2N} & \text{for all } \boldsymbol{\alpha}\in\mathcal{A}_2 \end{cases}$$

where $\rho(\theta)$ is the probability density over θ.

In other words, non-zero $\rho(\theta)$ gives contribution $\cos\theta\cos\frac{\pi}{2N}$ to the first integral, and $\sin\theta\cos\frac{\pi}{2N}$ to the second. In order that both integrals are equal, we should take $\rho(\theta)$ to be symmetric about $\theta=\frac{\pi}{8}$. For functions with this symmetry, non-zero $\rho(\theta)$ gives contribution $(\sin\theta+\cos\theta)\cos\frac{\pi}{2N}$ to both integrals. The minimum of this over $0\le\theta\le\frac{\pi}{8}$ is $\cos\frac{\pi}{2N}$, which occurs for $\theta=0$. It follows that the most experimentally challenging distribution to rule out is $\rho(\theta)=\frac{1}{2}(\delta_{\theta,0}+\delta_{\theta,\frac{\pi}{4}})$, where $\delta_{x,y}$ is the Kronecker delta (this being the distribution that requires the lowest measured δ_N to eliminate). For this distribution, we have $\max_{\boldsymbol{\alpha}}\langle|\boldsymbol{\alpha}\cdot\mathbf{z}|\rangle_{\mathbf{z}}/2=\frac{1}{4}\cos\frac{\pi}{2N}$, so this model is ruled out for $\max(\delta_N^1,\delta_N^2)<\delta_N^{\mathrm{crit4}}=\frac{1}{4}\cos\frac{\pi}{2N}$. Again, as detailed in Supplemental Table A1.1, our experimental data is sufficient to do so. (The lowest visibility that could rule out this case is 0.951, which would do so for $N=5$).

Note that, while discussing this case, we have so far ignored the requirement $\sum_z P_{\mathbf{Z}}(\mathbf{z})P_{X|\boldsymbol{\alpha}\mathbf{z}}=\frac{1}{2}$. However, this condition can be ensured (without changing the critical value $\delta_N^{\mathrm{crit4}}$) by replacing the probability density $\rho(\theta)$ with $\frac{1}{2}(\rho(\theta)+\rho(\pi+\theta))$, i.e. by distributing the density of each vector evenly between itself and the vector orthogonal to it.

Comment on minimum visibilities required to rule out Leggett models

Here we briefly compare the visibilities required to rule out Leggett models using our approach with those needed in previously considered Leggett inequalities. We remind the reader that the technique used in the present work generates conclusions that apply to arbitrary theories and were not developed with Leggett's model in mind. Nevertheless, use of this new approach to rule out Leggett models requires comparable visibilities to those of previously discussed inequalities. More specifically, the claimed minimum visibilities are 0.974 in Gröblacher *et al.* [13] and 0.943 for the alternative inequality of Branciard *et al.* [15, 16], which is only slightly below the value we require to rule out all of the four models above.

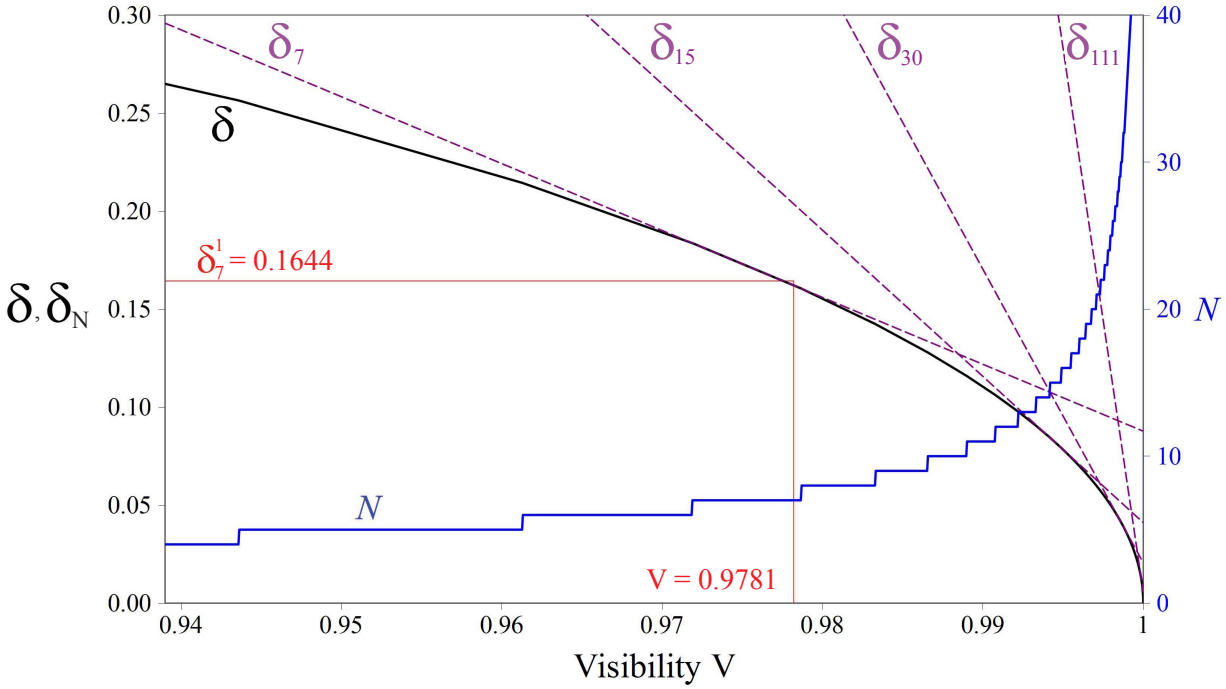
We note that the average visibility for measurements in the plane used in the main text was 0.9781 ± 0.0008, while the average visibility in the orthogonal plane (measured for the purposes of ruling out the second and fourth cases) was 0.9706 ± 0.0014.

III. VISIBILITY VERSUS δ

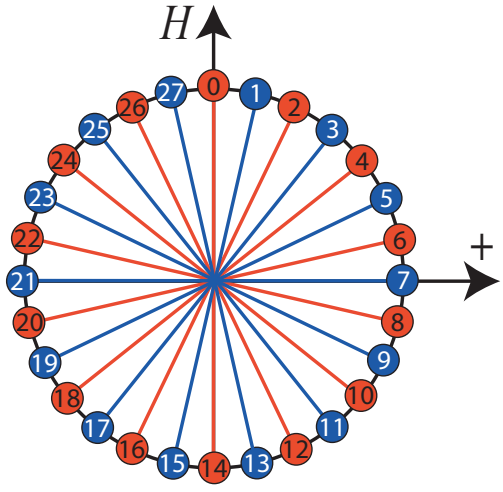
As discussed in the main manuscript, assuming the quantum theoretical predictions to be optimum, the minimum measurable value for δ_N, hence the bound on δ, depends on the quality of the generated bi-photon state and the measurement apparatus (characterized, e.g., through the visibility). This is depicted in Supplemental Figure A1.1 where, for simplicity, we assume a bias of zero (i.e. $\nu_N=0\ \forall\ N$). In order to decrease δ by more than a factor of two compared to our result, the average visibility on the measurement plane must exceed 0.995 (assuming zero bias and perfect measurement settings), and the required value of N increases to 15 or beyond, resulting in 120 or more high-precision coincidence measurements. To decrease δ below 1%, we require $V>0.9999$ and $N>111$. We emphasize that the precision required in the waveplate settings (that determine the spin measurements) increases with N, which rapidly constitutes another limitation to obtaining small values for δ, in addition to the need for a high-quality source.

IV. RAW DATA

The experimental settings as well as the associated measurement results that allow reconstruction of the density matrix are given in Supplemental Table A1.2. The most likely density matrix is detailed in Supplemental Table A1.3. Note that this density matrix is not used for the calculation of experimental values for δ_N, I_N or ν_N, but is included to characterize our source. The measurements settings used to experimentally determine δ_7 are depicted in Supplemental Figure A1.2, and Supplemental Table A1.4 lists the results used to calculate δ_7 from the bi-partite correlation I_7 and the bias ν_7.



Supplemental Fig. A1.1: δ **(minimum possible** δ_N**) and required number of bases per side** N **as a function of visibility** V**.** The stepped curve (N) uses the right y-axis. The curves are calculated using Werner states of varying visibility. The vertical and horizontal lines correspond to the average visibility for measurements in the plane used in the main text ($V = 0.9781$), and $\delta_7^1 = 0.1644$ respectively. The slight discrepancy between the intersection of these two lines and the curve showing $\delta(V)$ can be attributed to non-zero bias, imperfect measurements, and deviation of the experimental state from a Werner state. The dashed diagonal lines show δ_N as a function of visibility for $N = 7$, 15, 30, and 111. Note that, as $V \to 1$ and $\delta \to 0$, $N \to \infty$. Hence, significantly lowering δ requires not only higher visibilities than currently feasible [14, 15], but significantly more measurement settings (hence higher precision) also.



Supplemental Fig. A1.2: **Measurement settings for** $N = 7$**.** All settings are in the $|H\rangle$-$|+\rangle$ plane in the Bloch sphere. The settings on one side of the bipartite setup are indicated in red (even numbers) and those on the other side are indicated in blue (odd numbers).

Setting		HWP_A	QWP_A	HWP_B	QWP_B	R_C	ΔR_C
a	b	(°)	(°)	(°)	(°)	(cps)	(cps)
$\|H\rangle$	$\|H\rangle$	0	0	0	0	899.0	4.7
$\|H\rangle$	$\|V\rangle$	0	0	45	0	10.8	0.5
$\|H\rangle$	$\|+\rangle$	0	0	22.5	45	474.9	3.4
$\|H\rangle$	$\|-\rangle$	0	0	-22.5	45	463.0	3.4
$\|H\rangle$	$\|R\rangle$	0	0	0	45	464.5	3.4
$\|H\rangle$	$\|L\rangle$	0	0	0	-45	479.6	3.5
$\|V\rangle$	$\|H\rangle$	45	0	0	0	9.8	0.5
$\|V\rangle$	$\|V\rangle$	45	0	45	0	919.1	4.8
$\|V\rangle$	$\|+\rangle$	45	0	22.5	45	454.2	3.4
$\|V\rangle$	$\|-\rangle$	45	0	-22.5	45	451.9	3.4
$\|V\rangle$	$\|R\rangle$	45	0	0	45	461.1	3.4
$\|V\rangle$	$\|L\rangle$	45	0	0	-45	458.6	3.4
$\|+\rangle$	$\|H\rangle$	22.5	45	0	0	421.2	3.2
$\|+\rangle$	$\|V\rangle$	22.5	45	45	0	499.7	3.5
$\|+\rangle$	$\|+\rangle$	22.5	45	22.5	45	906.8	4.8
$\|+\rangle$	$\|-\rangle$	22.5	45	-22.5	45	17.7	0.7
$\|+\rangle$	$\|R\rangle$	22.5	45	0	45	443.0	3.3
$\|+\rangle$	$\|L\rangle$	22.5	45	0	-45	437.8	3.3
$\|-\rangle$	$\|H\rangle$	-22.5	45	0	0	507.5	3.6
$\|-\rangle$	$\|V\rangle$	-22.5	45	45	0	410.1	3.2
$\|-\rangle$	$\|+\rangle$	-22.5	45	22.5	45	22.2	0.7
$\|-\rangle$	$\|-\rangle$	-22.5	45	-22.5	45	902.3	4.7
$\|-\rangle$	$\|R\rangle$	-22.5	45	0	45	483.7	3.5
$\|-\rangle$	$\|L\rangle$	-22.5	45	0	-45	485.1	3.5
$\|R\rangle$	$\|H\rangle$	0	45	0	0	472.4	3.4
$\|R\rangle$	$\|V\rangle$	0	45	45	0	455.1	3.4
$\|R\rangle$	$\|+\rangle$	0	45	22.5	45	438.8	3.3
$\|R\rangle$	$\|-\rangle$	0	45	-22.5	45	469.9	3.4
$\|R\rangle$	$\|R\rangle$	0	45	0	45	19.1	0.7
$\|R\rangle$	$\|L\rangle$	0	45	0	-45	920.1	4.8
$\|L\rangle$	$\|H\rangle$	0	-45	0	0	484.3	3.5
$\|L\rangle$	$\|V\rangle$	0	-45	45	0	446.9	3.3
$\|L\rangle$	$\|+\rangle$	0	-45	22.5	45	456.0	3.4
$\|L\rangle$	$\|-\rangle$	0	-45	-22.5	45	491.3	3.5
$\|L\rangle$	$\|R\rangle$	0	-45	0	45	935.4	4.8
$\|L\rangle$	$\|L\rangle$	0	-45	0	-45	21.4	0.7

Supplemental Table A1.2: **Tomographic Data.** This table shows raw data collected to find the density matrix shown in Supplemental Table A1.3. The coincidence rates between the Si avalanche photodiode (APD) and the triggered 1550 nm InGaAs APD (R_C) for each set of photon analyzer settings are given in average counts per second (cps), as are their one standard deviation uncertainties (ΔR_C). Settings a and b were implemented using one quarter wave plate followed by one half wave plate in each analyzer. These waveplates were set at angles HWP_A, QWP_A, HWP_A, and QWP_A. Data collection time for each point was 30 seconds.

(a) ρ_{Re}

	$\langle HH\|$	$\langle HV\|$	$\langle VH\|$	$\langle VV\|$
$\|HH\rangle$	0.5031	0.0056	-0.0196	0.4828
$\|HV\rangle$	0.0056	0.0033	0.0006	0.0113
$\|VH\rangle$	-0.0196	0.0006	0.0032	-0.0115
$\|VV\rangle$	0.4828	0.0113	-0.0115	0.4904

(b) ρ_{Im}

	$\langle HH\|$	$\langle HV\|$	$\langle VH\|$	$\langle VV\|$
$\|HH\rangle$	0.0000	0.0020	0.0046	-0.0007
$\|HV\rangle$	-0.0020	0.0000	0.0002	-0.0012
$\|VH\rangle$	-0.0046	-0.0002	0.0000	-0.0036
$\|VV\rangle$	0.0007	0.0012	0.0036	0.0000

Supplemental Table A1.3: **Density matrix.** The real and imaginary parts of the density matrix generated by maximum likelihood quantum state tomography.

Setting		HWP_A	HWP_B	R_{Si}	R_C	$1-P(m,n)$	$P(m,n)$	$\Delta P(m,n)$	ν	$\Delta\nu$
m	n	(°)	(°)	(cps)	(cps)					
0	13	0	41.79	41885	10.6					
0	27	0	86.79	41825	546.0					
14	27	45	86.79	41908	12.5	0.0207	0.9793	0.0007	0.0008	0.0002
14	13	45	41.79	42068	544.3					
0	1	0	3.21	41847	545.2					
0	15	0	48.21	41855	9.2					
14	15	45	48.21	41954	547.9	0.9836	0.0164	0.0006	0.0011	0.0002
14	1	45	3.21	42121	9.1					
2	1	6.43	3.21	41826	540.5					
2	15	6.43	48.21	41871	11.4					
16	15	51.43	48.21	42028	552.5	0.9798	0.0202	0.0007	0.0013	0.0002
16	1	51.43	3.21	42102	11.1					
2	3	6.43	9.64	41829	546.3					
2	17	6.43	54.64	41880	11.5					
16	17	51.43	54.64	42024	544.2	0.9781	0.0219	0.0007	0.0006	0.0002
16	3	51.43	9.64	41886	12.9					
4	3	12.86	9.64	41871	541.0					
4	17	12.86	54.64	41806	13.4					
18	17	57.86	54.64	41929	543.0	0.9745	0.0255	0.0007	0.0009	0.0002
18	3	57.86	9.64	42037	15.0					
4	5	12.86	16.07	41739	545.4					
4	19	12.86	61.07	41757	11.4					
18	19	57.86	61.07	41975	555.4	0.9779	0.0221	0.0007	0.0013	0.0002
18	5	57.86	16.07	41967	13.5					
6	5	19.29	16.07	41595	541.2					
6	19	19.29	61.07	41776	17.5					
20	19	64.29	61.07	42043	548.8	0.9717	0.0283	0.0008	0.0023	0.0002
20	5	64.29	16.07	42109	14.2					
6	7	19.29	22.5	41752	548.7					
6	21	19.29	67.5	41805	12.5					
20	21	64.29	67.5	42181	548.1	0.9760	0.0240	0.0007	0.0022	0.0002
20	7	64.29	22.5	42121	14.6					
8	7	25.71	22.5	41886	540.4					
8	21	25.71	67.5	41907	14.3					
22	21	70.71	67.5	42189	549.7	0.9727	0.0273	0.0008	0.0016	0.0002
22	7	70.71	22.5	42143	16.3					
8	9	25.71	28.93	41763	548.9					
8	23	25.71	73.93	41795	12.9					
22	23	70.71	73.93	42180	545.4	0.9737	0.0263	0.0008	0.0023	0.0002
22	9	70.71	28.93	42135	16.7					
10	9	32.14	28.93	42097	554.4					
10	23	32.14	73.93	42260	14.1					
24	23	77.14	73.93	42038	548.7	0.9744	0.0256	0.0007	0.0008	0.0002
24	9	77.14	28.93	42055	14.9					
10	11	32.14	35.36	42039	554.5					
10	25	32.14	80.36	42306	12.2					
24	25	77.14	80.36	42063	557.4	0.9768	0.0232	0.0007	0.0005	0.0002
24	11	77.14	35.36	42116	14.3					
12	11	38.57	35.36	42515	556.4					
12	25	38.57	80.36	42325	14.0					
26	25	83.57	80.36	41993	544.0	0.9753	0.0247	0.0007	0.0025	0.0002
26	11	83.57	35.36	42005	13.1					
12	13	38.57	41.79	42281	534.4					
12	27	38.57	86.79	42324	9.4					
26	27	83.57	86.79	41879	535.9	0.9825	0.0175	0.0007	0.0022	0.0002
26	13	83.57	41.79	41985	9.7					

Supplemental Table A1.4: **Raw Data used to calculate δ_7^1.** This table shows raw data collected to find $\delta_7^1 = 0.1644 \pm 0.0014$. $HWP_{A/B}$ are the half wave-plate settings that realize the measurements corresponding to m and n as shown in Supplemental Figure A1.2. The Si APD rates (R_{Si}) and the coincidence rates between the Si APD and the triggered InGaAs APD (R_C) are both given in average cps. $P(m,n)$ is the probability of correlated outcomes and ν is the bias for individual measurements as detailed in the Methods section. Data collection time for each point was 40 seconds. Uncertainties are one standard deviation.

[1] Colbeck, R. & Renner, R. No extension of quantum theory can have improved predictive power. *Nature Communications* **2**, 411 (2011).
[2] Chen, Z. & Montina, A. Measurement contextuality is implied by macroscopic realism. *Physical Review A* **83**, 042110 (2011).
[3] Bell, J. S. Free variables and local causality. In *Speakable and unspeakable in quantum mechanics*, chap. 12 (Cambridge University Press, 1987).
[4] Pearle, P. M. Hidden-variable example based upon data rejection. *Physical Review D* **2**, 1418–1425 (1970).
[5] Braunstein, S. L. & Caves, C. M. Wringing out better Bell inequalities. *Annals of Physics* **202**, 22–56 (1990).
[6] Pomarico, E., Bancal, J.-D., Sanguinetti, B., Rochdi, A. & Gisin, N. Various quantum nonlocality tests with a commercial two-photon entanglement source. *Physical Review A* **83**, 052104 (2011).
[7] Barrett, J., Hardy, L. & Kent, A. No signalling and quantum key distribution. *Physical Review Letters* **95**, 010503 (2005).
[8] Barrett, J., Kent, A. & Pironio, S. Maximally non-local and monogamous quantum correlations. *Physical Review Letters* **97**, 170409 (2006).
[9] Colbeck, R. & Renner, R. Hidden variable models for quantum theory cannot have any local part. *Physical Review Letters* **101**, 050403 (2008).
[10] de Broglie, L. La mécanique ondulatoire et la structure atomique de la matière et du rayonnement. *Journal de Physique, Serie VI* **VIII**, 225–241 (1927).
[11] Bohm, D. A suggested interpretation of the quantum theory in terms of "hidden" variables. I. *Physical Review* **85**, 166–179 (1952).
[12] Leggett, A. J. Nonlocal hidden-variable theories and quantum mechanics: An incompatibility theorem. *Foundations of Physics* **33**, 1469–1493 (2003).
[13] Gröblacher, S. *et al.* An experimental test of non-local realism. *Nature* **446**, 871–875 (2007).
[14] Paterek, T. *et al.* Experimental test of nonlocal realistic theories without the rotational symmetry assumption. *Physical Review Letters* **99**, 210406 (2007).
[15] Branciard, C. *et al.* Experimental falsification of Leggett's non-local variable model. *Physical Review Letters* **99**, 210407 (2007).
[16] Branciard, C. *et al.* Testing quantum correlations versus single-particle properties within Leggett's model and beyond. *Nature Physics* **4**, 681–685 (2008).
[17] Suarez, A. Why aren't quantum correlations maximally nonlocal? Biased local randomness as essential feature of quantum mechanics. e-print `arXiv:0902.2451` (2009).

Supplemental Material: Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks

A. Rubenok,[1] J. A. Slater,[1] P. Chan,[2] I. Lucio-Martinez,[1] and W. Tittel[1]

[1]*Institute for Quantum Science & Technology and Department of Physics & Astronomy, University of Calgary, Canada*
[2]*Institute for Quantum Science & Technology and Department of Electrical & Computer Engineering, University of Calgary, Canada*

I. ENSURING INDISTINGUISHABILITY

In order to ensure the indistinguishability of photons arriving at Charlie's and to allow Bell state measurements in a real-world environment, we developed and implemented three stabilization systems (see Fig. 2 in the main text): fully-automatic polarization stabilization, manual adjustment of photon arrival time, and manual adjustment of laser frequency. Note that automating the frequency and timing stabilization systems is straightforward, particularly if the active control elements are placed in Charlie's setup.

The polarization stabilization system [1, 2] employed an additional laser (at Charlie's) and two polarization controllers (one at Alice's and one at Bob's). Every 10 s, Charlie disabled data collection for 0.5 s and sent high intensity, vertically polarized stabilization light to Alice and Bob. This light was detected by photodiodes at Alice's and Bob's, and used to trigger their commercially available polarization controllers (POCs), which were programmed to adjust the polarization of the stabilization light to vertical. This implies that Alice's and Bob's attenuated laser pulses, which were emitted horizontally polarized, both arrive horizontally polarized at Charlie's.

To stabilize the frequency difference between Alice's and Bob's lasers, Alice used a frequency shifter (FS) that employed a linear phase chirp via a serrodyne modulation signal applied to a phase modulator. Whenever the error rate in the *x-key* increased significantly, Charlie communicated the frequency difference after measuring the beat frequency by mixing their unmodulated and unattenuated laser outputs on the beam splitter. Adjustments, in the worst case, were required every 30 minutes to maintain the difference below 10 MHz.

To enable temporal synchronization, Charlie sent a master clock signal via a second set of fibers to Alice and Bob. Roughly every minute, Charlie measured the qubit arrival-time difference using his SPDs and high-resolution electronics and sent this information to Alice and Bob. They then adjusted their qubit generation times using function generators to apply a phase shift to the recovered master clock. This maintained the arrival-time difference under 30 ps.

II. DECOY-STATE ANALYSIS

In MDI-QKD the secret key rate is given by

$$S \geq Q_{11}^{z}\big(1 - h_2(e_{11}^{x})\big) - Q_{\mu\sigma}^{z} f h_2(e_{\mu\sigma}^{z}), \tag{1}$$

where $h_2(X)$ denotes the binary entropy function evaluated on X, and f describes the efficiency of error correction with respect to Shannon's noisy coding theorem. Furthermore, Q_{11}^{z}, e_{11}^{x}, $Q_{\mu\sigma}^{z}$, and $e_{\mu\sigma}^{z}$ are gains (Q – the probability of a projection onto $|\psi^{-}\rangle$ per emitted pair of pulses) and error rates (e – the ratio of erroneous to total projections onto $|\psi^{-}\rangle$) in either the x- or z-basis for Alice and Bob sending single photons (denoted by subscript "11"), or for pulses emitted by Alice and Bob with mean photon number μ and σ (denoted by subscript "$\mu\sigma$"), respectively. While $Q_{\mu\sigma}^{z}$, and $e_{\mu\sigma}^{z}$ are directly accessible from experimental data, Q_{11}^{z}, e_{11}^{x} have to be bounded using a decoy state method.

We use a three-intensity decoy state method for the MDI-QKD protocol [3] that derives a lower bound for Q_{11}^{x} and Q_{11}^{z} and an upper bound for e_{11}^{x}, to calculate a lower bound for the secure secret key rate. We denote the signal, decoy, and vacuum intensities by μ_s, μ_d, and μ_v, respectively, for Alice, and Bob (note that $\mu_v = 0$ by definition). In our implementation Alice and Bob both select the same mean photon numbers for the three intensities and use channels of equal transmission. For compactness of notation, we omit the μ when describing the gains and error rates (e.g. we write Q_{ss}^{z} to denote the gain in the z-basis when Alice and Bob both send photons using the signal intensity). Under these assumptions, the lower bound on Q_{11}^{x} is given by

$$Q_{11}^{x} \geq \frac{P_1(\mu_s)P_2(\mu_s)\big(Q_{dd}^{x} - Q_0^{x}(\mu_d)\big) - P_1(\mu_d)P_2(\mu_d)\big(Q_{ss}^{x} - Q_0^{x}(\mu_s)\big)}{P_1(\mu_s)P_1(\mu_d)\big(P_1(\mu_d)P_2(\mu_s) - P_1(\mu_s)P_2(\mu_d)\big)}, \tag{2}$$

where the various $P_i(\mu)$ denote the probabilities that a pulse with Poissonian photon number distribution and mean μ contains exactly i photons, and $Q_0^z(\mu_d)$ and $Q_0^z(\mu_s)$ are given by

$$Q_0^x(\mu_d) = P_0(\mu_d)Q_{vd}^x + P_0(\mu_d)Q_{dv}^x - P_0(\mu_d)^2 Q_{vv}^x, \quad (3)$$
$$Q_0^x(\mu_s) = P_0(\mu_s)Q_{vs}^x + P_0(\mu_s)Q_{sv}^x - P_0(\mu_s)^2 Q_{vv}^x. \quad (4)$$

Similar equations are used to bound Q_{11}^z (we replace the superscript x by z). Finally, the error rate e_{11}^x can then be computed as

$$e_{11}^x \leq \frac{e_{dd}^x Q_{dd}^x - P_0(\mu_d)e_{vd}^x Q_{vd}^x - P_0(\mu_d)e_{dv}^x Q_{dv}^x + P_0(\mu_d)^2 e_{vv}^x Q_{vv}^x}{P_1(\mu_d)^2 Q_{11}^x}, \quad (5)$$

where the upper bound holds if a lower bound is used for Q_{11}^x. Note that $Q_{11}^{x,z}$, $Q_0^{x,z}(\mu_d)$, $Q_0^{x,z}(\mu_s)$ and e_{11}^x (Eqs. 2-5) are uniquely determined through measurable gains and error rates.

Our analysis in [4] determined that lowering μ_d as much as possible maximizes secret key rate. In these experiments, we select $\mu_d = 0.05$ in order to obtain statistically significant data in a reasonable amount of time (see Suplementary Table A2.1)

III. SECURE KEY DISTRIBUTION USING MDI-QKD

In this section we describe the assumptions underpinning secure key distribution in MDI-QKD as well as further technological and theoretical developments required for our current proof-of-principle demonstration to meet this goal. We note that any QKD system used to distribute secret key must be vetted against attacks arising from imperfections in its implementation[1]. Protection against such attacks requires the development of hardware that strives to be as ideal as possible, in conjunction with the development of security proofs that are able to take into account those imperfections that inevitably remain in any realistic implementation. (Such proofs would bound the information leaked to an eavesdropper, which, in turn, allows removing it by means of privacy amplification). Even for the heavily studied prepare-and-measure BB84 protocol, this is an area of ongoing research [6], and more needs to be done for the new MDI-QKD protocol. Yet, MDI-QKD constitutes a very important development in this context as it eliminates all potential attack strategies related to imperfections in the measurement apparatus, including arbitrary measurement-basis misalignment errors as well as detector attacks that have recently been shown to provide the eavesdropper full information about the key without leaving a trace [7–10]. Remaining assumptions and required developments are:

1. **Quantum mechanics is correct and complete.** This assumption is generally believed to be true.

2. **Alice's and Bob's laboratories are private.** This assumption entails that no undesired signals, e.g. RF electromagnetic radiation, escape from Alice's and Bob's apparatus when working in normal conditions. Information gain through such passive observation can be avoided using appropriate shielding, which, as is standard in academic QKD implementations, we have not spent any particular effort on. Furthermore, the assumption implies that Eve cannot actively obtain information about the experimental settings, e.g. by sending a probe, such as light, into the laboratories using the fiber that connects Alice or Bob, respectively, with the outside world, and analyzing the back reflection. This is often referred to as a Trojan horse attack [11, 12]. And finally, Eve cannot actively influence Alice's or Bob's devices to modify their functioning. Protection against active attacks requires that the laboratories are isolated from signals sent by Eve, e.g. using optical isolators or attenuators. No such countermeasures were realized in our proof-of-principle demonstration. However, their implementation is straightforward, at least in what concerns attenuators and isolators [13]. We emphasize that there is no need to protect Charlie's laboratory; the MDI-QKD protocol ensures that it can even be run by the eavesdropper.

3. **Alice and Bob send phase-randomized attenuated pulses of light produced by a laser operated well above threshold.** This ensures that the generated light pulses are correctly described by the density

[1] A notable exception is fully device independent QKD (DI-QKD) [5], which, however, is currently impossible to realize due to the need for a loophole free violation of a Bell inequality.

TABLE A2.1: List of experimentally obtained error rates, $e^{x,z}_{\mu\sigma}$, and gains, $Q^{x,z}_{\mu\sigma}$, used to calculate the secret key rate in four different configurations. For each configuration we show the mean photon numbers for the signal and decoy states, μ_s and μ_d, employed by Alice and Bob. The vacuum state corresponds to a mean photon number of $\mu_v = 0$. We remind the reader that we omit the μ when writing the gains and error rates, writing only the subscript denoting the signal (s), decoy (d), or vacuum (v) state. We also indicate the lengths of fiber connecting Alice and Charlie (ℓ_A), Bob and Charlie (ℓ_B) and the total transmission loss (l). Finally, the computed secret key rate (S) is shown in bits per detector gate. Additionally, we measured $Q^{x,z}_{vv} = (7.1 \pm 0.30) \times 10^{-10}$ and $e^{x,z}_{vv} = 0.49 \pm 0.021$, which is applied to all distances.

Fiber	Spool	Z-basis				X-basis			
ℓ_A	22.85 km	Q^z_{ss}	$1.028(3) \times 10^{-4}$	e^z_{ss}	0.0311(4)	Q^x_{ss}	$1.95(1) \times 10^{-4}$	e^x_{ss}	0.270(2)
ℓ_B	22.55 km	Q^z_{sv}	$2.98(5) \times 10^{-6}$	e^z_{sv}	0.49(1)	Q^x_{sv}	$5.68(2) \times 10^{-5}$	e^x_{sv}	0.494(2)
Total loss l	9.1 dB	Q^z_{vs}	$1.78(4) \times 10^{-6}$	e^z_{vs}	0.47(1)	Q^x_{vs}	$5.77(2) \times 10^{-5}$	e^x_{vs}	0.507(2)
μ_s	0.396(4)	Q^z_{dd}	$1.89(3) \times 10^{-6}$	e^z_{dd}	0.070(4)	Q^x_{dd}	$3.40(1) \times 10^{-6}$	e^x_{dd}	0.277(2)
μ_d	0.050(1)	Q^z_{dv}	$1.05(6) \times 10^{-7}$	e^z_{dv}	0.47(3)	Q^x_{dv}	$8.76(8) \times 10^{-7}$	e^x_{dv}	0.511(5)
S	$1.4(4) \times 10^{-6}$	Q^z_{vd}	$9.24(5) \times 10^{-8}$	e^z_{vd}	0.48(3)	Q^x_{vd}	$8.59(9) \times 10^{-7}$	e^x_{vd}	0.503(5)

Fiber	Spool	Z-basis				X-basis			
ℓ_A	30.98 km	Q^z_{ss}	$1.67(1) \times 10^{-5}$	e^z_{ss}	0.041(2)	Q^x_{ss}	$3.57(3) \times 10^{-5}$	e^x_{ss}	0.274(3)
ℓ_B	34.65 km	Q^z_{sv}	$6.7(2) \times 10^{-7}$	e^z_{sv}	0.51(2)	Q^x_{sv}	$9.62(9) \times 10^{-6}$	e^x_{sv}	0.498(4)
Total loss l	13.7 dB	Q^z_{vs}	$4.4(2) \times 10^{-7}$	e^z_{vs}	0.48(2)	Q^x_{vs}	$9.32(7) \times 10^{-6}$	e^x_{vs}	0.499(4)
μ_s	0.279(6)	Q^z_{dd}	$6.0(1) \times 10^{-7}$	e^z_{dd}	0.082(5)	Q^x_{dd}	$1.192(7) \times 10^{-6}$	e^x_{dd}	0.278(2)
μ_d	0.050(1)	Q^z_{dv}	$4.7(4) \times 10^{-8}$	e^z_{dv}	0.47(4)	Q^x_{dv}	$3.08(7) \times 10^{-7}$	e^x_{dv}	0.50(1)
S	$1.7(1.3) \times 10^{-7}$	Q^z_{vd}	$4.0(4) \times 10^{-8}$	e^z_{vd}	0.41(4)	Q^x_{vd}	$3.03(7) \times 10^{-7}$	e^x_{vd}	0.50(1)

Fiber	Spool	Z-basis				X-basis			
ℓ_A	40.80 km	Q^z_{ss}	$5.57(6) \times 10^{-6}$	e^z_{ss}	0.053(2)	Q^x_{ss}	$9.87(9) \times 10^{-6}$	e^x_{ss}	0.270(4)
ℓ_B	40.77 km	Q^z_{sv}	$2.15(9) \times 10^{-7}$	e^z_{sv}	0.51(2)	Q^x_{sv}	$2.50(3) \times 10^{-6}$	e^x_{sv}	0.505(7)
Total loss l	18.2 dB	Q^z_{vs}	$1.88(8) \times 10^{-7}$	e^z_{vs}	0.49(2)	Q^x_{vs}	$2.95(4) \times 10^{-6}$	e^x_{vs}	0.501(6)
μ_s	0.251(6)	Q^z_{dd}	$2.66(6) \times 10^{-7}$	e^z_{dd}	0.129(8)	Q^x_{dd}	$4.49(4) \times 10^{-7}$	e^x_{dd}	0.286(4)
μ_d	0.050(1)	Q^z_{dv}	$2.8(2) \times 10^{-8}$	e^z_{dv}	0.52(4)	Q^x_{dv}	$1.25(4) \times 10^{-7}$	e^x_{dv}	0.51(1)
S	$1.2(8) \times 10^{-7}$	Q^z_{vd}	$2.2(2) \times 10^{-8}$	e^z_{vd}	0.45(4)	Q^x_{vd}	$1.22(3) \times 10^{-7}$	e^x_{vd}	0.51(1)

Fiber	Deployed	Z-basis				X-basis			
ℓ_A	12.4 km	Q^z_{ss}	$1.042(3) \times 10^{-4}$	e^z_{ss}	0.0323(6)	Q^x_{ss}	$2.020(8) \times 10^{-4}$	e^x_{ss}	0.265(2)
ℓ_B	6.2 km	Q^z_{sv}	$2.96(6) \times 10^{-6}$	e^z_{sv}	0.50(1)	Q^x_{sv}	$5.63(2) \times 10^{-5}$	e^x_{sv}	0.492(2)
Total loss l	9.0 dB	Q^z_{vs}	$1.87(4) \times 10^{-6}$	e^z_{vs}	0.52(1)	Q^x_{vs}	$5.10(2) \times 10^{-5}$	e^x_{vd}	0.512(2)
μ_s	0.402(2)	Q^z_{dd}	$1.82(2) \times 10^{-6}$	e^z_{dd}	0.071(3)	Q^x_{dd}	$3.35(2) \times 10^{-6}$	e^x_{dd}	0.269(3)
μ_d	0.050(1)	Q^z_{dv}	$1.15(6) \times 10^{-7}$	e^z_{dv}	0.53(3)	Q^x_{dv}	$8.5(1) \times 10^{-7}$	e^x_{dv}	0.502(6)
S	$1.5(5) \times 10^{-6}$	Q^z_{vd}	$8.4(5) \times 10^{-8}$	e^z_{vd}	0.49(4)	Q^x_{vd}	$8.5(1) \times 10^{-7}$	e^x_{vd}	0.501(6)

matrix $\rho = \sum_n P_n(\mu)|n\rangle\langle n|$, where $P_n(\mu) = \frac{e^{-\mu}\mu^n}{n!}$ is the Poisson distribution with mean photon number μ, and $|n\rangle\langle n|$ denotes the density matrix of an n-photon Fock state. This condition is easily met by generating every light pulse using a laser diode triggered by a short electrical pulse. However, as we carve qubits out of a laser beam with large coherence time using an intensity modulator, it is not fulfilled in our setup (more precisely, subsequent pulses are coherent). Yet, we point out that the solution to our problem is well understood and has been implemented before [14]: it simply requires adding a phase modulator that randomizes the global phase of each qubit.

4. **The mean values of photons per pulse, as well as the encoded states are chosen randomly.** No random choices have been implemented in our current proof-of-principle demonstration. Instead, we sent pulses with the same mean photon number and encoded the same qubit state during several minutes before changing the state or mean number. However, operating the phase and amplitude modulators that generate qubit states using adequate drivers connected to quantum random number generators is well understood [13], and meeting the requirement of random modulation is straightforward, though time consuming.

5. **Alice and Bob generate qubits in states that are sufficiently close to those that form two maximally conjugate bases.** These states were denoted in the main text as $|0\rangle$, $|1\rangle$, $|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, respectively. This assumption may currently not be satisfied (see [4] for a detailed description

of our experimental imperfections). For instance, considering states in different bases (for which the overlap should be 0.5), we find an average deviation of 0.074, and for different states in the same basis (for which we expect an overlap of zero), the average deviation is 0.013. According to the analyses in [3, 15] these overlaps, together with the current detector performance, are insufficient to securely distribute key. However, we point out that both proofs lead to very conservative bounds. For instance, the proof in [3] requires a state generation procedure that artificially increases error rates and applies non-tight bounds, and hence underestimates secure key rates. We believe that future investigations will rapidly improve proof techniques and yield higher secret key rates (and result in secret key in cases in which current proofs predict no secret key). Furthermore, we note that straightforward technological improvements allow reducing the maximum deviation from the ideal overlap values to around 1 part in 1000. For instance, this can be accomplished by reducing ringing in our pulse generation by a factor of 5, and using commercially-available, state-of-the-art intensity modulators that allow suppressing the background by an additional 10-20 dB [16]. In addition, using state-of-the-art detectors with 93% quantum efficiency and 1kHz noise [17] leads, according to simulation results with a theoretical model of MDI-QKD that we presented in [4], to secret key rates similar to or above the ones reported in the main document, even using the conservative approach in [3].

6. **Sufficiently weak correlations between qubit states and all degrees of freedom not used to encode the qubit.** In principle, the various states generated by Alice and Bob could have differences in other degrees of freedom (i.e. polarization, spectral, spatial, or temporal modes), which could open a security loophole [18] if not properly quantified and taken into account during privacy amplification. However, for MDI-QKD, the link between correlations with unobserved degrees of freedom and Eve's information gain is not yet clear. In particular, correlations are likely to degrade the visibility of the BSM, thus creating observable errors. The upper bound on Eve's information gain, possibly zero, can only be assessed using plausible arguments based on the actual implementation of the setup supplemented by careful measurements. For instance, in our implementation, the use of a single laser to generate all qubits states and of a single-mode fiber to transmit qubits from Alice, or Bob, to Charlie, respectively, makes it highly unlikely that correlation between states and photon spectra or spatial modes exist. Furthermore, careful programming of the function generator that generates all states through interaction with the same intensity modulator makes it very plausible that no temporal distinguishability is observable in our experiment. And finally, the polarization beam splitter at the exit of Alice's and Bob's laboratories ensures equal polarization of all time-bin qubit states.

7. **Appropriate classical post-processing of the sifted key, i.e. error correction and privacy amplification**. Note that while we have not implemented error correction, we have used a realistic estimation of the error correction efficiency [13] to determine the potential secret key rate of our system. Furthermore, we did not consider finite key size effects in our proof-of-principle demonstration (in other words, we assumed that we could run our QKD devices during an infinitely long time and produce an infinite amount of measured data), which, in the case of MDI-QKD, have so far only been investigated using an overly conservative approach [19].

8. **A short secret authentication key exists before starting QKD.** This key is used to authenticate the classical communication channel during error correction and privacy amplification. As we did not implement any of these post-processing steps, we did not need any pre-established secret key. In an actual implementation, this step can, for instance, be accomplished during a personal meeting between Alice and Bob.

We recall that some of the above topics are currently not as thoroughly studied for MDI-QKD as for prepare-and-measure QKD. However, the ability to close all side channels in measurement devices represents a significant step forward in closing the gap between theoretical security proofs and experimentally viable implementations. In particular, it has, for the first time, allowed for the development of security proofs in QKD that take arbitrary state generation and measurement errors into account, even though the efficiency of the current approaches can certainly be increased[2]. In addition, for actual key distribution, our experimental implementation has to be improved along the lines discussed above. We leave these interesting and important topics for future investigations and emphasize that our work has focused on previously undemonstrated requirements for MDI-QKD, such as the Bell state measurement over deployed fiber, on improving the understanding of the capabilities and current limitations of our setup (including optimization and efficiency calculations of a decoy state analysis; for more information see [4]) and on experimental demonstrations of the protocol over various distances as well as over deployed, real-world optical fiber.

---

[2] In comparison, the only security proof for BB84 QKD dealing with arbitrary state generation errors at the source and arbitrary misalignment of the measurement bases is limited to individual attacks but does not apply to more powerful coherent attacks [6].

IV. DISCUSSION OF ERROR RATES $e^{x,z}_{\mu\sigma}$

Let us briefly discuss the ideal case in which the quantum states encoded into attenuated laser pulses, as well as the projection measurements, are perfect. To gain some insight into how the difference in the error rates, $e^{x,z}_{\mu\sigma}$, arises[3], we consider only the most likely case that can cause the detection pattern associated with a projection onto $|\psi^-\rangle$ (this projection occurs if the two detectors indicate detections with 1.4±0.4 ns time difference). Specifically, we consider only the case in which two photons arrive at the beam splitter. Note that these photons can either come from the same person, or from different persons.

- z-basis: Assuming that Alice and Bob both prepare states in the z-basis, only photons prepared in orthogonal states can cause a projection onto $|\psi^-\rangle$. This implies that one photon has to come from Alice, and the other one from Bob (if generated by the same person, both photons would be in the same state). Hence, taking into account Bob's bit flip, Alice and Bob always establish identical bits, i.e. $e^z_{\mu\sigma}(\text{ideal}) = 0$.

- x-basis: Assuming that both Alice and Bob prepare states in the x-basis, it is no longer true that only photons prepared in orthogonal states and by different persons can cause a projection onto $|\psi^-\rangle$. Indeed, if the two photons have been prepared by the same person, it is possible to observe the detection pattern associated with a projection onto $|\psi^-\rangle$. In this case, given that all detected photons have been prepared by either one or the other person, the detection does not indicate any correlation between the states prepared by Alice and Bob. In turn, this leads to uncorrelated key bits. Thus, $e^x_{\mu\sigma}(\text{ideal})$ is determined by the probability that one photon arrived from each person relative to the probability that two photons arrived from the same person. A detailed analysis for attenuated laser pulses with Poissonian photon number distribution, assuming an equal probability of photons arriving from either party, yields $e^x_{\mu\sigma}(\text{ideal}) = 1/4$.

---

[1] I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier and W. Tittel, Proof-of-concept of real-world quantum key distribution with quantum frames. *New J. Phys.* **11,** 095001 (2009).
[2] F. Bussières, J. A. Slater, J. Jin, N. Godbout and W. Tittel, Testing nonlocality over 12.4 km of underground fiber with universal time-bin qubit analyzers. *Phys. Rev. A* **81**, 052106 (2010).
[3] X.-B. Wang, Three-intensity decoy state method for device independent quantum key distribution with basis dependent errors. *arXiv:1207.0392* (2012).
[4] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez and W. Tittel, Modelling MDI-QKD. http://arxiv.org/abs/1204.0738.
[5] L. Masanes, S. Pironio and A. Acín, Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Communications* **2,** 238 (2011).
[6] E. Woodhead and S. Pironio, Effects of preparation and measurement misalignments on the security of the BB84 quantum key distribution protocol. *arXiv:1209.6479* (2012).
[7] A. Lamas-Linares and C. Kurtsiefer, Breaking a quantum key distribution system through a timing side channel, *Opt. Express*, **15** (15), 9388-9393 (2007).
[8] 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,** 042333 (2008).
[9] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics* **4,** 686689 (2010).
[10] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Thermal blinding of gated detectors in quantum cryptography. *Opt. Express* **18** (26), 27938-27954 (2010).
[11] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Quantum cryptography. *Rev. Mod. Phys.* **74,** 145-195 (2002).
[12] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus and M. Peev, The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301-1350 (2009).
[13] M. Sasaki *et al.* Field test of quantum key distribution in the Tokyo QKD Network. Opt. Express **19** (11), 10387-10409 (2011).
[14] Y. Zhao, B. Qi and H.-K. Lo, Experimental quantum key distribution with active phase randomization, *Appl. Phys. Lett.*, **90** (4), 044106 (2007).

---

[3] Note when two superscripts, each one denoting a different basis, are present on variables, (e.g. $e^{x,z}_{\mu\sigma}$, as above, or $Q^{x,z}_{\mu\sigma}$), this is a shorthand for, e.g. $e^z_{\mu\sigma}$ and $e^x_{\mu\sigma}$ – that is, the statement is valid for both the z- and x-bases. Note that variables may take different values for each basis, e.g. $e^z_{\mu\sigma} \neq e^x_{\mu\sigma}$. When this notation is used within an equation such as Eq. **??**, then the equation may be written for either the z- or x-basis.

[15] K. Tamaki, H.-K. Lo, C.-H. F. Fung and B. Qi, Phase encoding schemes for measurement device independent quantum key distribution and basis-dependent flaw. *arXiv:1111.3413* (2012).
[16] http://www.eospace.com
[17] F. Marsili *et al.* Detecting Single Infrared Photons with 93% System Efficiency. *arXiv:1209.5774* (2012).
[18] S. Nauerth *et al.* Information leakage via side channels in freespace BB84 quantum cryptography. *New J. Phys.* **11,** 065001 (2009).
[19] T.-T. Song, Q.-Y. Wen, F.-Z. Guo and X.-Q. Tan, Finite-key analysis for measurement-device-independent quantum key distribution, Phys. Rev. A **86**, 022332 (2012).

Two-photon interference of weak coherent laser pulses recalled from separate solid-state quantum memories

Jeongwan Jin,[1] Joshua A. Slater,[1] Erhan Saglamyurek,[1] Neil Sinclair,[1] Mathew George,[2] Raimund Ricken,[2] Daniel Oblak,[1] Wolfgang Sohler,[2] and Wolfgang 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]*Department of Physics - Applied Physics, University of Paderborn, Warburger Strasse 100, 33095 Paderborn, Germany*

Supplementary Information

A. Properties of waveguide $LiNbO_3$ crystal and AFC.

In the experimental configuration in which the HOM-interference occurs between two pulses recalled from separate quantum memories we pointed, in the main text, to the different properties of the two memory devices. In this section we wish to elaborate on the differences between the two memories based on their physical dissimilarity and measured optical depth as a function of frequency. Memory waveguide a is 10.4 mm long and crystal b is 15.4 mm long. The optical depths at 795.43 nm are around 2.5 and 3.2 for waveguide a and b, respectively, as shown by the light-grey curves in Fig. A3.1 a,b, corresponding to the case in which the memories are not activated.

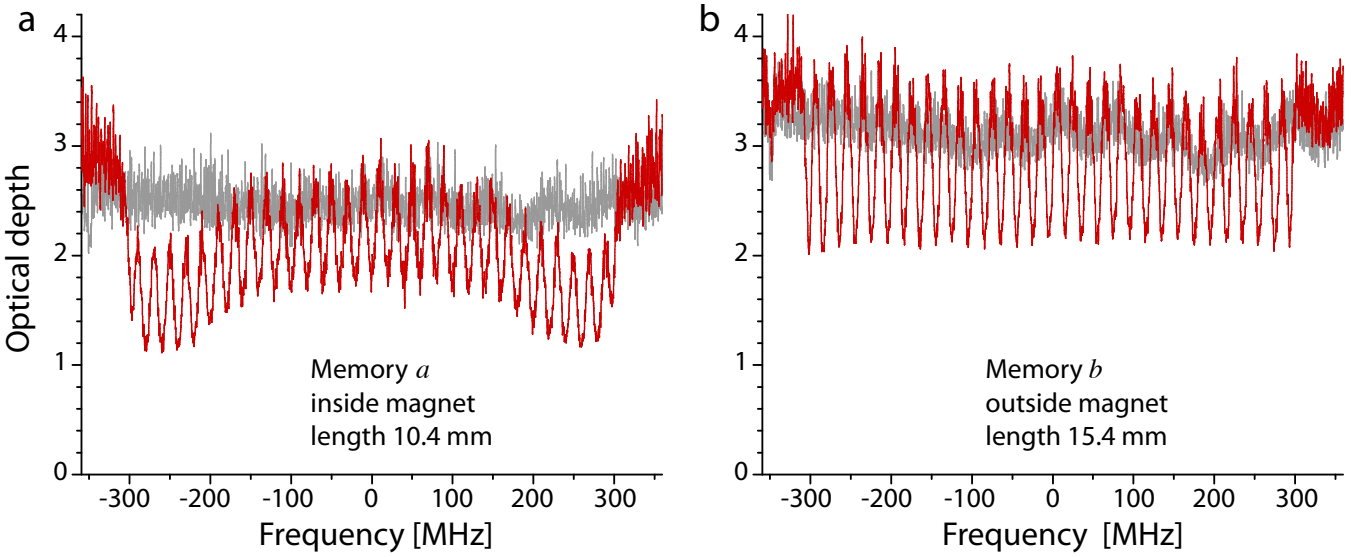


FIG. A3.1: Measured optical depths of our two Ti:Tm:$LiNbO_3$ waveguides as a function of frequency shift of the probing light imparted by the phase-modulator. Light grey traces show optical depths when the memories are inactive, i.e. no AFC is prepared. Dark red traces show the prepared AFCs at a magnetic field of 900 Gauss at the centre of the solenoid.

In order to spectrally tailor an AFC in Tm:$LiNbO_3$, a magnetic field must be applied along the crystal's c-axis so as to split the ground and excited level multiplets into their two nuclear Zeeman sublevels[1]. However, as one crystal is located at the centre of the setup's solenoid and the other outside the solenoid (see Fig. 2 in the main text) it is not possible to apply the same B-field at the two crystals. Thus when we activate both memories we generally apply a magnetic field, which provides a reasonable balance in recall efficiencies but is not optimal for either memory. This circumstance is reflected by the different shapes of optical-depth profiles of the AFCs shown in red in Fig. A3.1a,b.

B. Two-photon interference in imperfectly prepared memories.

In all our demonstrations of the HOM interference we consistently observe that the HOM visibility is close to the theoretical maximum for coherent states. Yet, it is important to realize that an improperly configured AFC quantum

memory does alter a stored photon's wavefunction, resulting in imperfect HOM interference with a non-stored photon.

To support this claim we activate only memory a, whose performance we change by varying the bandwidth of the AFC, and interfere the recalled pulses with pulses directly transmitted through the deactivated memory b. As the AFC bandwidth decreases below that of the probe pulses, the AFC effectively acts as a bandpass filter for the stored photons and we thus expect the recalled pulses to be temporally broadened w.r.t. the original pulse. This is observed in the insert of Fig. A3.2, which shows smoothed histograms of photon detection events as a function time. It is worth noting that the small bandwidth AFC also acts as a bandpass filter for the transmitted pulse by virtue of the different effective optical depths inside and outside the AFC. Thus the broadened transmitted pulse starts to overlap with the echo for the narrow AFC bandwidth traces, as is also observed in the insert of Fig. A3.2.

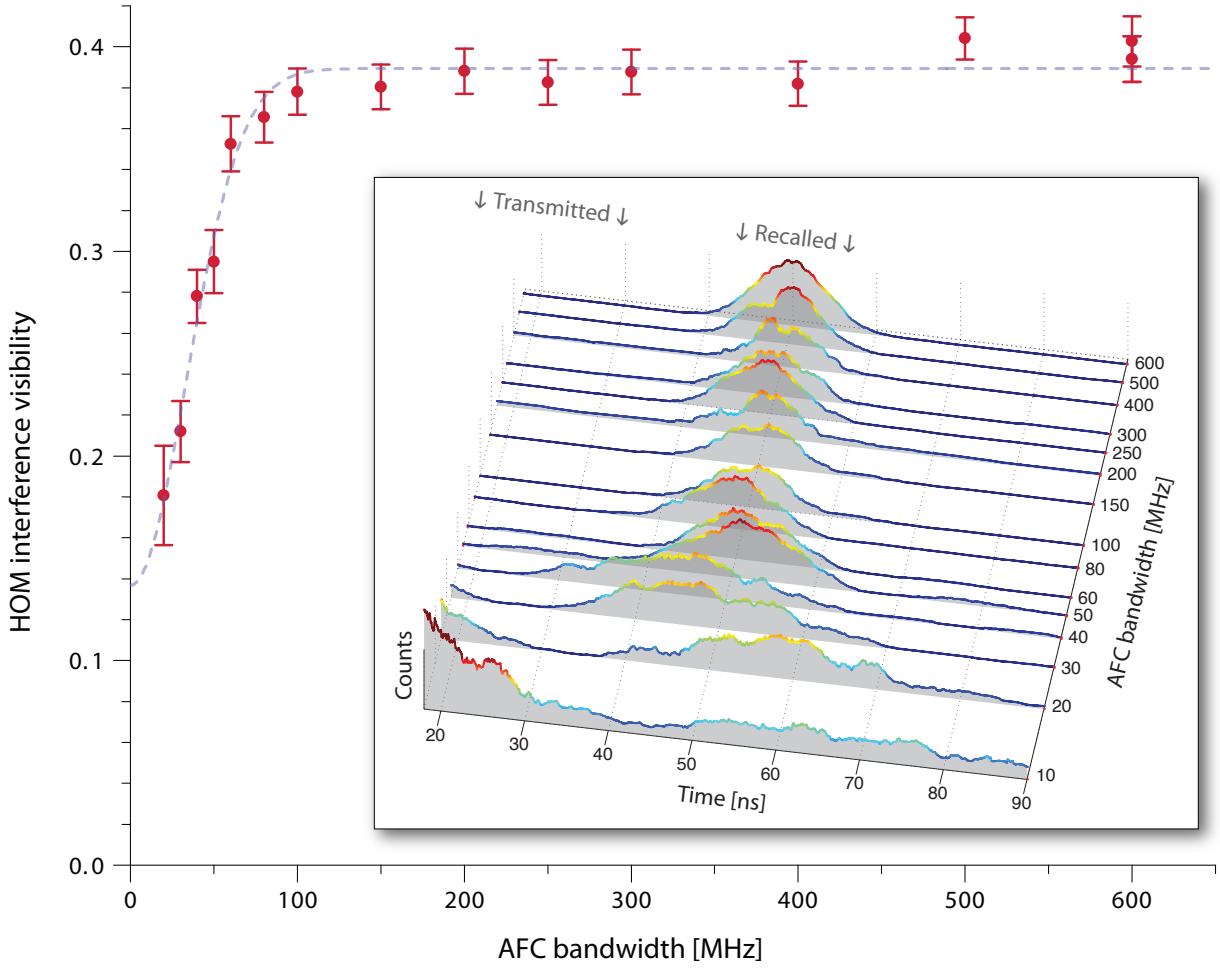


FIG. A3.2: HOM interference visibility if HOM-BS input pulses are recalled from AFCs with varying bandwidths. Insert: Histograms of recalled pulse detection times for different AFC bandwidths clearly showing broadening of recalled (and transmitted) pulses for bandwidths below 100 ns.

Another consequence of reducing the AFC bandwidth is that the overall efficiency of the quantum memory decreases, which causes an imbalance between the mean photon numbers at the HOM-BS inputs and thus reduces HOM interference visibility. We circumvent the change to the echo efficiency by adapting the mean photon number at the memory input so as to keep the mean photon number of the recalled pulse constant. With this remedial procedure, we assess the HOM visibility by changing the HOM-BS inputs from parallel to orthogonal polarizations for a series of different AFC bandwidths. The HOM visibility in Fig. A3.2 is steady for bandwidths from around 100 MHz and up. However, below 100 MHz the visibility begins to drop significantly. The dashed line is a fit of the visibilities to a Gaussian function with full-width at half-maximum (FWHM) of $79 \pm 4\ MHz$. Note, that the reason for the visibility being limited to around 40% is solely that, for this measurement, we do not go through the usual careful optimization steps.

With these measurements we have illustrated how a quantum memory could alter the photonic wavefunction resulting in a reduced HOM interference visibility. A combination of spectral and temporal distortion of the photonic

wavefunction is indeed a common type of perturbation by quantum memories.[2, 3] It is particularly worth noting that the gradient-echo memory (GEM) quantum memory protocol, though similar to the AFC protocol, imparts a frequency chirp to the recalled pulse[4]. If not corrected, this feature constitutes a perturbation of the wavefunction of the recalled pulse, which may render it unsuitable for applications relying on two-photon interference.

C. Analytical model of second-order interference in coincidence measurements.

In the following theoretical treatment we will derive expressions for the coincidence and single-detector counts in terms of probabilities. By multiplying these probabilities with the average experimental repetition rate we can easily calculate the predicted experimental count rates. To a large extent though, we will mainly be interested in relative probabilities or count rates between different settings of the degrees of freedom of pulses.

It is reasonably straightforward to derive the rates of detection of photons at the outputs of a BS (note that in this Supplementary Information, the HOM-BS of the main text will be referred to as just BS) In our case coherent states $|\alpha\rangle$ and $|\beta\rangle$, characterized by mean photon numbers $\langle\hat{a}^\dagger\hat{a}\rangle = |\alpha|^2$ and $\langle\hat{b}^\dagger\hat{b}\rangle = |\beta|^2$, occupy the two spatial input modes of the BS. In the Fock-basis the coherent state can be represented as

$$|\alpha\rangle = \sum_{n=0}^{\infty} e^{-\frac{|\alpha|^2}{2}} \frac{\alpha^n}{\sqrt{n!}}|n\rangle = \sum_{n=0}^{\infty} e^{-\frac{|\alpha|^2}{2}} \frac{\alpha^n}{n!}(\hat{a}^\dagger)^n|0\rangle, \tag{1}$$

and similarly for $|\beta\rangle$.

To account for the cases of photons being distinguishable and indistinguishable at the BS we must allow for an additional degree of freedom in each of the spatial modes, e.g. polarization, frequency, or time. Thus we write the input state at one of the BS inputs as $|\alpha_1,\, \alpha_2\rangle \equiv |\alpha_1\rangle \otimes |\alpha_2\rangle$, where α_1 and α_2 are the coherent state amplitudes in the two orthogonal modes of the auxiliary degree of freedom within the same spatial mode. We treat the coherent state at the other BS input in a similar way.

For the case in which the fields at the inputs of the BS are distinguishable with respect to the auxiliary degree of freedom, the inputs to the BS are described as being in the state $|\alpha,\, 0\rangle|0,\, \beta\rangle \equiv |\alpha,\, 0\rangle \otimes |0,\, \beta\rangle$, whereas in the case of them being indistinguishable (up to a difference in the mean photon number) the input fields are written as $|\alpha,\, 0\rangle|\beta,\, 0\rangle$.

The BS is characterized by its reflection amplitude r and transmission amplitude $t = \sqrt{1-|r|^2}$, which cause the input creation operators to transform as $\hat{a}^\dagger \rightarrow t\hat{c}^\dagger + ir\hat{d}^\dagger$ and $\hat{b}^\dagger \rightarrow ir\hat{c}^\dagger + t\hat{d}^\dagger$. With this in hand, we can compute the state in the BS outputs for any combination of Fock states at the inputs. When the two input states are indistinguishable, i.e. in the same auxiliary degree of freedom, we get[5]

$$\begin{aligned} |n,0\rangle|m,0\rangle \rightarrow & \sum_{j=0}^{n}\sum_{k=0}^{m} K_{\parallel}(n,m,j,k)\,|j+k,\,0\rangle|n+m-j-k,\,0\rangle \\ & K_{\parallel}(n,m,j,k) = t^{m-k+j}(ir)^{n-j+k}\sqrt{\binom{n}{j}\binom{m}{k}\binom{j+k}{j}\binom{n+m-j-k}{n-j}}, \end{aligned} \tag{2}$$

where the binomial coefficient $\binom{x}{y} = \frac{x!}{y!(x-y)!}$. For distinguishable input fields the output state is slightly simpler

$$\begin{aligned} |n,0\rangle|0,m\rangle \rightarrow & \sum_{j=0}^{n}\sum_{k=0}^{m} K_{\perp}(n,m,j,k)\,|j,\,k\rangle|n-j,\,m-k\rangle \\ & K_{\perp}(n,m,j,k) = \sum_{j=0}^{n}\sum_{k=0}^{m} t^{m-k+j}(ir)^{n-j+k}\sqrt{\binom{j}{k}\binom{n-j}{m-k}}. \end{aligned} \tag{3}$$

The above calculated output modes impinge on the single photon detectors (SPDs). These may be characterized by the probability of detecting an incident single photon. From this single photon detection probability η it is also possible to deduce the probability of detecting a pulse consisting of multiple photons, keeping in mind that, irrespective of the number of photons, only a single detection event can be generated. We write $p_1(n)$ for the probability for generating one detector event given n incident photons, and it is useful to note that it relates to the probability $p_0(n)$ of detecting nothing as $p_1(n) = 1 - p_0(n)$. The probability for not detecting n photons is, on the other hand, easily computed as $p_0(n) = (1-\eta)^n$. Since the two detectors at the BS outputs are independent, the probability $p_{11}(n,m)$ of generating

a coincidence event, i.e. having simultaneous detection events in each of the detectors, given n and m photons in one and the other output is simply $p_{11}(n,m) = p_1(n)p_1(m)$. Thus the probability for a coincidence detection becomes

$$p_{11}(n,m) = [1-(1-\eta_1)^n]\,[1-(1-\eta_2)^m]\,, \tag{4}$$

where η_1 and η_2 are the single photon detection probabilities for detector 1 and 2, respectively. Expressing the coincidence detection probability in terms of Fock states at the BS input we have

$$\begin{aligned} P_{11}^{\parallel}(n,m) &= \sum_{j=0}^{n}\sum_{k=0}^{m} |K_{\parallel}(n,m,j,k)|^2 \; p_{11}(j+k,\, n+m-j-k) \\ &= \sum_{j=0}^{n}\sum_{k=0}^{m} |K_{\parallel}(n,m,j,k)|^2 \; \left[1-(1-\eta_1)^{j+k}\right]\left[1-(1-\eta_2)^{n+m-j-k}\right]\,, \end{aligned} \tag{5}$$

where $K_{\parallel}(n,m,j,k)$ should be substituted with the factor from Eq. (2). For distinguishable inputs we find a similar expression for $P_{11}^{\perp}(n,m)$ using the factor $K_{\perp}(n,m,j,k)$ from Eq. (3). It is assumed that the detector at a given spatial output mode is equally sensitive to photons in both auxiliary modes, i.e. it detects the states $|k,\, j\rangle$ and $|j,\, k\rangle$ with equal probability.

We are now in the position to formulate an expression for the different detection probabilities given a particular set of coherent input fields. The probability to generate a detection event in both detectors, given coherent input fields of amplitudes α and β, is

$$\mathcal{P}_{11}^{\parallel(\perp)}(\alpha,\beta) = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} e^{-|\alpha|^2-|\beta|^2}\,\frac{(\alpha^n\beta^m)^2}{n!\,m!}\,P_{11}^{\parallel(\perp)}(n,m)\,. \tag{6}$$

(Note that to distinguish the probability in Eq. (5), which is applicable to Fock states, from that inEq. (6), which applies to coherent state inputs, we use P to denote the former and $\mathcal{P}$ for the latter.) This allows us to derive the visibility of the HOM interference on the two detectors as

$$\mathcal{V}_{11}(\alpha,\beta,\eta_1,\eta_2,r) = \frac{\mathcal{P}_{11}^{\perp}(\alpha,\beta) - \mathcal{P}_{11}^{\parallel}(\alpha,\beta)}{\mathcal{P}_{11}^{\perp}(\alpha,\beta)}\,, \tag{7}$$

where we have spelled out the parameters that affect the value of the visibility. The quantity $\mathcal{V}_{11}$ is referred to as the *HOM visibility*.

D. Simplified model for HOM visibility.

To gain some intuitive understanding of the way the HOM visibility is affected by the experimental parameters we resort to a couple of approximations. Firstly, we assume equal mean photon numbers at the inputs of the beam-splitter, $|\alpha|^2 = |\beta|^2 \equiv \mu$, the BS ratio to be 50:50 (i.e. $r = t = 1/\sqrt{2}$), and the detectors to have equal single photon detection probability $\eta_1 = \eta_2 \equiv \eta$. Secondly, since we normally work at very low mean photon numbers $\mu < 1$ only the first couple of terms of Eq. (1) need to be included. Specifically, we Taylor expand $e^{-\mu/2}$ and keep only terms in the sum up to 2^{nd} order in μ. Thus, for the coincidence detection events we get the probabilities

$$\mathcal{P}_{11}^{\parallel} = \eta^2\frac{\mu^2}{2} \tag{8}$$

$$\mathcal{P}_{11}^{\perp} = \eta^2\mu^2\,, \tag{9}$$

which results in a HOM visibility of

$$\mathcal{V}_{11} = \frac{1}{2}\,. \tag{10}$$

A key point is that the HOM visibility of 50% is independent of the mean photon number μ. This observation can be explained by noting that in this low order treatment the coincidences in the case of indistinguishable input modes stem mostly from events in which two photons are present at the same input, which occurs with probability $p_0p_2 + p_2p_0$. For distinguishable input modes the coincidences stem from all events that contain two photons at the input, i.e. $p_1p_1 + p_0p_2 + p_2p_0$. Since, according to Eq. (1), for coherent input states, all of these probabilities scale in the same way with the mean photon number, their ratio, and thus the visibility of Eq. (7), is constant for all mean photon numbers.

E. Compilation of experimental results for HOM interference at the few-photon level.

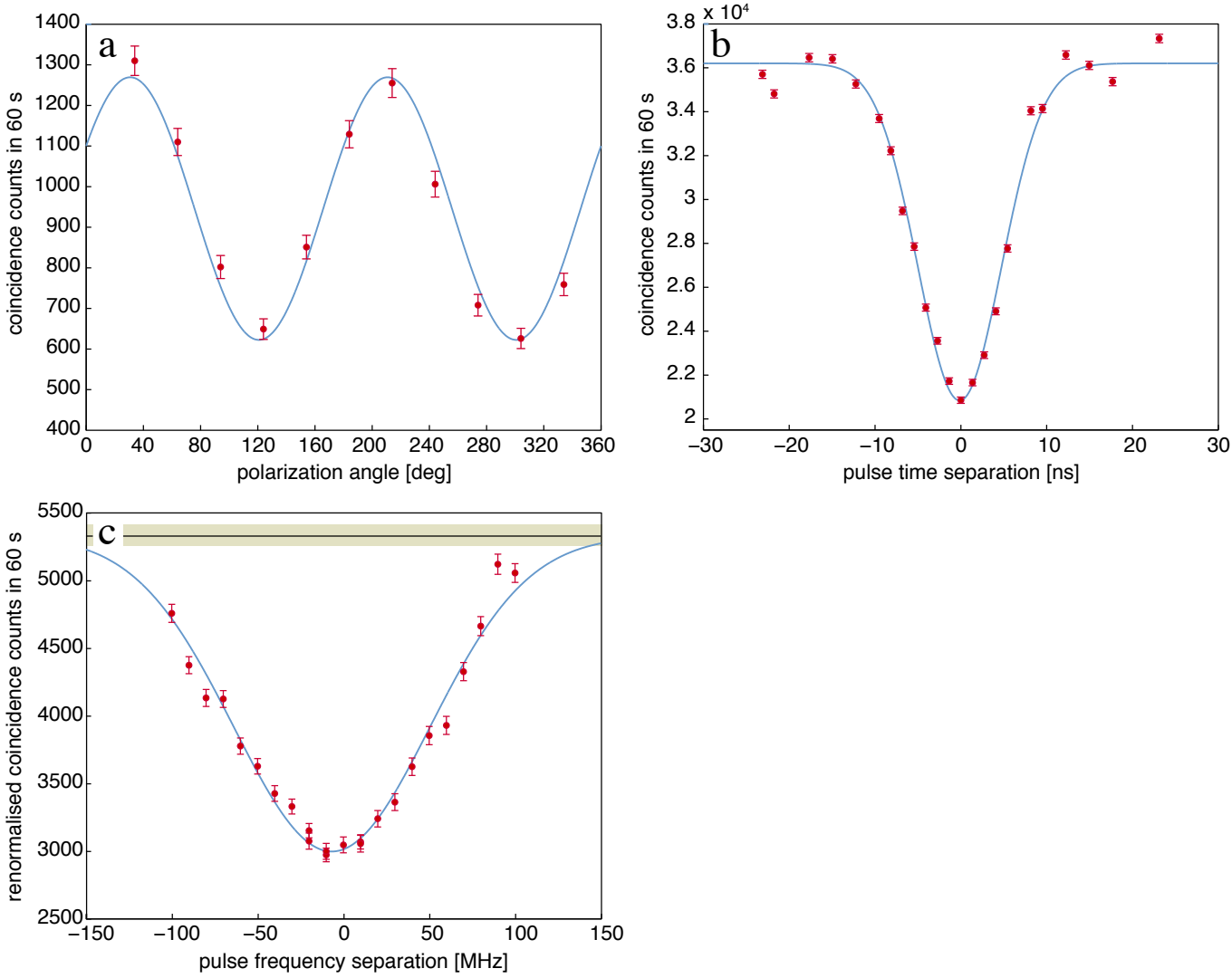


FIG. A3.3: HOM interference manifested in coincidence counts between BS outputs with inactive memories. a) Changing the polarization angle between the pulses yields a HOM visibility of $\mathcal{V} = 50.96 \pm 5.56\%$. b) Varying the temporal overlap of the pulses produces $\mathcal{V} = 42.43 \pm 2.27\%$. c) Altering the frequency overlap of the pulse spectra results in $\mathcal{V} = 43.72 \pm 1.70\%$.

Here we show the plots of coincidence count rates on which the few-photon values in Table 1 of the main text are based. We restate that coincidence count rates are proportional to coincidence probabilities by a factor that is given by the average experimental repetition rate. Moreover, when calculating the HOM visibility, only the relative probabilities or count rates in a measurement are important. In the experiments we change the mutual polarization, time separation, or frequency difference of the pulses at the BS (in the main text referred to as HOM-BS) input as explained in the Methods.

Deactivated memories: We present the data in order of the number of activated memories starting with none, i.e. pulses merely pass through attenuated to the BS. In Fig. A3.3a) we show the coincidence counts as we vary the polarization difference of the pulses at the two inputs of the BS. Fitting the data to a sine function we obtain a visibility of $\mathcal{V} = 50.96 \pm 5.56\%$. In Fig. A3.3b) we display the coincidence counts as we step the temporal separation of the pulses at the two inputs of the BS. The count rates for these measurements are generally higher than all the other count rates presented. This is because this data was acquired by looking at coincidences between the transmitted part of the probe pulses in the configuration of two active quantum memories (shown in Fig. A3.5b)). Hence, the balancing of the mean photon number in the transmitted pulses done less meticulously, which is the most likely reason for the observed lower visibility of $\mathcal{V} = 42.43 \pm 2.27\%$ in this case.

Fig. A3.3c) shows the coincidence count rates as function of the frequency difference of the two pulses at the BS inputs. The horizontal line and surrounding shaded band shown in Fig. A3.3c) – as well as in Fig. A3.4c) – give the coincidence counts for completely distinguishable input photons as obtained by making the polarizations orthogonal. As noted in the Methods, it is necessary to resort to the polarization degree of freedom in order to make the pulses completely distinguishable. The visibility from the fit is noticeably lower than that obtained when we change the other degrees of freedom. There are two main reasons for this. The first is that, in order to generate pulses with different frequencies, we drive the AOM at the limits of its bandwidth. This, in turn, necessitates setting the RF drive signal amplitude high whereby the frequency purity of the signal is contaminated by higher-order harmonics. Although it is not expected to change the maximal interference value occurring when the pulses are generated with the same modulation frequency, it will alter the shape of the interference as a function of the pulse frequency difference. Hence, the fitted Gaussian curve, assuming a Fourier limited pulse, may not correctly reproduce the actual frequency dependence of the interference. Indeed, the minimum coincidence rates consistently fall below the fitted curve. A second factor reducing the observed visibility is related to the need to adjust the AOM drive amplitude to balance the bandwidth limitation. The limited accuracy with which we are able to estimate the appropriate RF amplitude results in significant scattering of the coincidence counts due to variations in input pulse intensities. To amend this we have found that it is necessary to normalize the points to the count rates on the individual detectors, as indicated on the y-axis of plot Fig. A3.4c. Unfortunately, the manifestation of the HOM interference in the single-detector count rates – which will be elaborated later in the Supplementary Information – means that such a normalization procedure tends to reduce the visibility in the coincidence counts.

One active memory: Next in line are the plots for the case in which only memory a is activated, while the other is left inactive. In Fig. A3.4 we present the coincidence count rates when changing the same degrees of freedom as in case of both memories being inactive. Additionally, in Fig. A3.4d, we plot the coincidence count rates when changing the storage time in the quantum memory.

Two active memories: Lastly, we present the plots for the case in which both memories are activated. Due to limitations in our current setup it is not possible to simultaneously generate two quantum memories with different storage times, and therefore we do not acquire a storage time scan when both memories are active. Furthermore, we skip the characterization with respect to the spectral degree of freedom. The coincidence count data for the remaining two degrees of freedom are plotted in Fig. A3.5, which also includes the appropriate fits.

F. Manifestation of HOM interference in single detector counts.

We also evaluate the effect of the two-photon interference on the counts registered by a single detector. This is easily done by amending the detection probability to the case of one detection event in one detector and any number of events x (i.e. $x = 0, 1$) in the other detector. We arrive at

$$p_{1x}(n, m) = 1 - (1 - \eta_1)^n \,. \tag{11}$$

This expression can be inserted into Eq. (5) to calculate $P_{1x}^{\|(\perp)}(n, m)$, which, through Eq. (6), gives us $\mathcal{P}_{1x}^{\|(\perp)}(\alpha, \beta)$, and from which the *single-detector visibility* $\mathcal{V}_{1\mathrm{x}}$ is defined analogous to Eq. (7).

We can formulate a simplified expression by using the same approximations as in the case of coincidence detections:

$$\mathcal{P}_{1x}^{\|} = \eta\mu + \eta\left(2 - \frac{3\eta}{4}\right)\mu^2 \tag{12}$$

$$\mathcal{P}_{1x}^{\perp} = \eta\mu + \eta\left(2 - \frac{\eta}{2}\right)\mu^2 \,, \tag{13}$$

from which we get the single-detector visibility

$$\mathcal{V}_{1\mathrm{x}} = \frac{\eta\mu}{4 + 2(4 - \eta)\mu} \,. \tag{14}$$

In the limit of low detector efficiency, $\mathcal{V}_{1\mathrm{x}} \approx 0$, since, in that case, the probability of detecting two photons impinging on the detector is simply twice that of detecting one. This nulls the limitation that only a single detection event can be generated per pulse. Furthermore, the single-detector visibility also goes to zero for very low mean photon numbers. In this case it is very unlikely to have two photons either at the *same* or at *different* input ports of the BS, hence most of the single detector counts stem from single photons from either one or the other input of the BS. It is interesting to note that if η is known for a detector, then, from observing the single-detector visibility (see Eq. (14)), it is in principle possible to estimate the mean photon number per pulse μ.

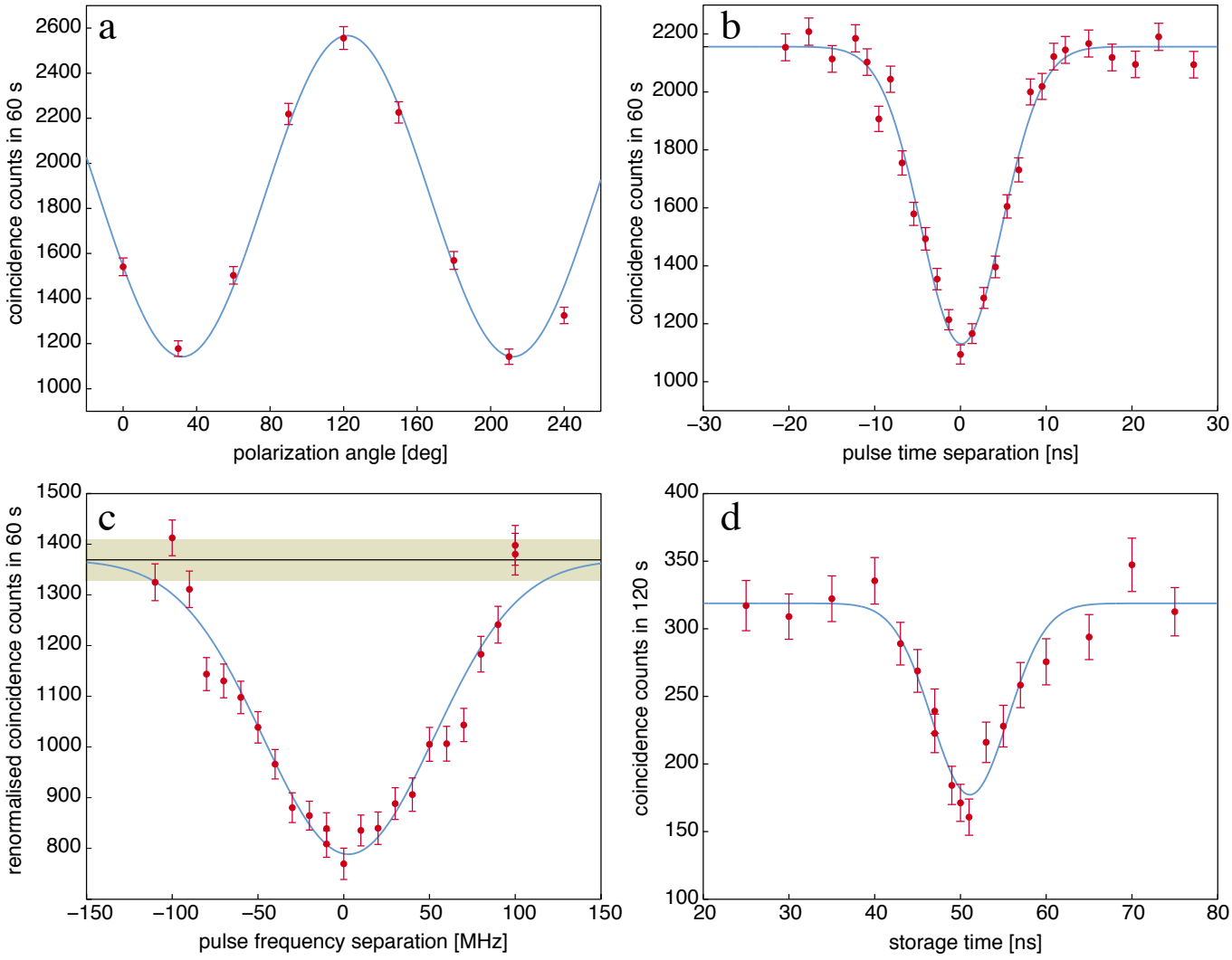


FIG. A3.4: HOM interference manifested in coincidence counts between BS outputs with one active memory. a) Changing the polarization angle between the pulses yields a HOM visibility of $\mathcal{V} = 55.51 \pm 4.09\%$. b) Varying the temporal overlap of the pulses produces $\mathcal{V} = 47.57 \pm 2.96\%$. c) Altering the frequency overlap of the pulse spectra results in $\mathcal{V} = 42.40 \pm 3.51\%$. d) Varying the storage time of the quantum memory and thus the temporal overlap of the pulses yields $\mathcal{V} = 44.4 \pm 6.9\%$.

Another important consequence of the manifestation of two-photon interference in the single-detector counts is that the single-detector counts cannot generally be used to normalize the coincidence counts w.r.t. fluctuations in the input pulse intensities. Only for detectors with low detection efficiency or very low mean photon numbers, in which case $\mathcal{V}_{1x} \approx 0$, is this normalization possible.

G. Experimental results on HOM interference manifested in single-detector counts

First, in Figure A3.7, we present the single-detector counts corresponding to the coincidence counts depicted in Figure A3.4a,b. In the case where we vary the polarization and time separation we see a clear change in the single-detector counts, which, moreover, is evidently correlated with the change in coincidence counts. The count variation due to the two-photon interference is somewhat masked by the single-detector count scatter, which is due to intensity fluctuations mainly in the light going through the 10 km delay line. We fit the data in Figures A3.7a and b with a sine and Gaussian function, respectively. For the former we find a mean photon number of $\mu = 0.52$ while from the latter we estimate $\mu = 0.54$. From the number of single-detector counts there is some evidence to conclude that the light intensity is about 15% higher. To this should be added about 25% uncertainty for the intensity at the BS w.r.t.

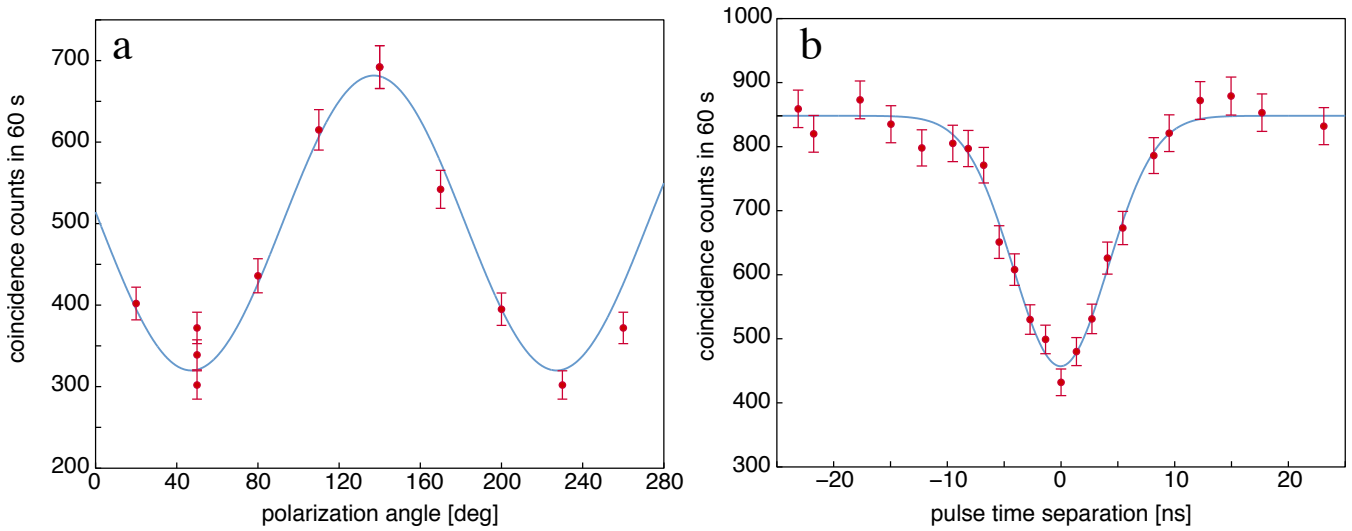


FIG. A3.5: HOM interference manifested in coincidence counts between BS outputs with two active memories. a) Changing the polarization angle between the pulses yields a HOM visibility of $\mathcal{V} = (53.1 \pm 5.3)\%$. b) Varying the temporal overlap of the pulses produces $\mathcal{V} = (46.1 \pm 3.2)\%$.

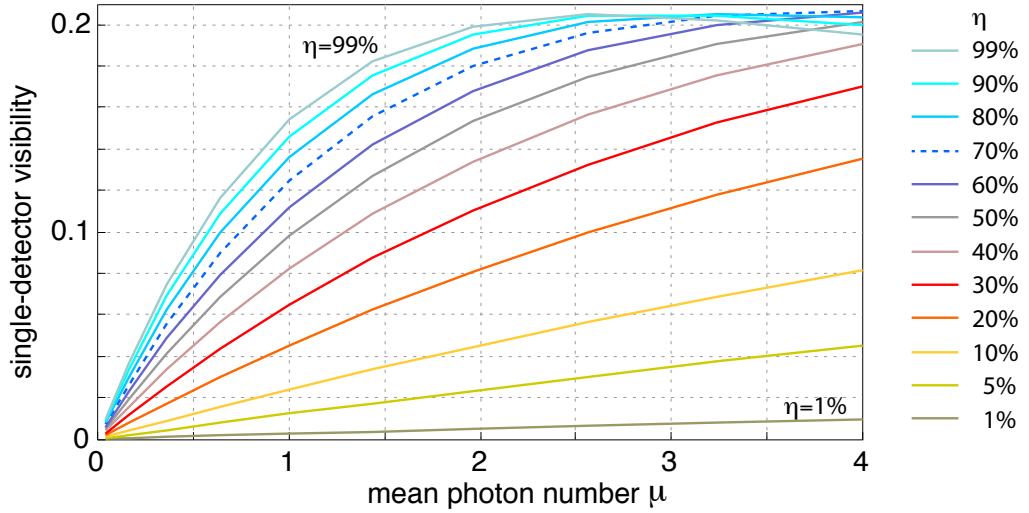


FIG. A3.6: Plots of single-detector visibility as a function of the mean photon number for detectors with a range of single photon detection probabilities η. The $\eta = 70\%$ trace, highlighted with a dashed line, corresponds approximately to our detectors, which have $65\% \leq \eta \leq 75\%$.

the intensity at the detector due to variation in the loss in the fibre mating sleeves. Finally, the scatter of the counts makes the fits themselves rather uncertain. Nevertheless, the mere fact that the two-photon interference is manifested in the single-detector counts validates the order of magnitude of the mean photon number, as depicted in Fig. A3.6.

Figure A3.8 depicts the single-detector counts corresponding to the coincidence counts depicted in Figure A3.5a,b. Again, from fitting the appropriate functions to the polarization and time data yields visibilities around 7%, corresponding to mean photon numbers of around $\mu = 0.5$.

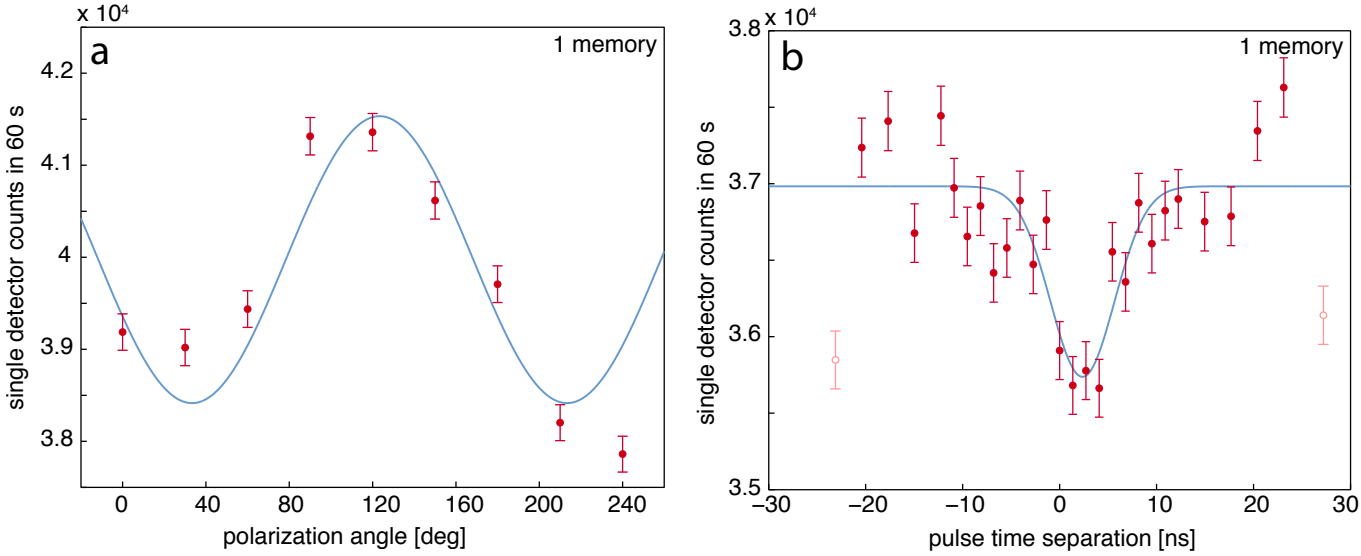


FIG. A3.7: HOM interference manifested in single-detector counts in the case of one active quantum memory when changing a) polarization and b) time difference between pulses at BS input. For the polarization scan in a) we find $\mathcal{V}_{1x} = (7.51 \pm 3.80)\%$ and for the time scan in b) we get $\mathcal{V}_{1x} = (7.75 \pm 3.25)\%$. For this measurement we only recorded the single-detector counts from Si-APD 1.

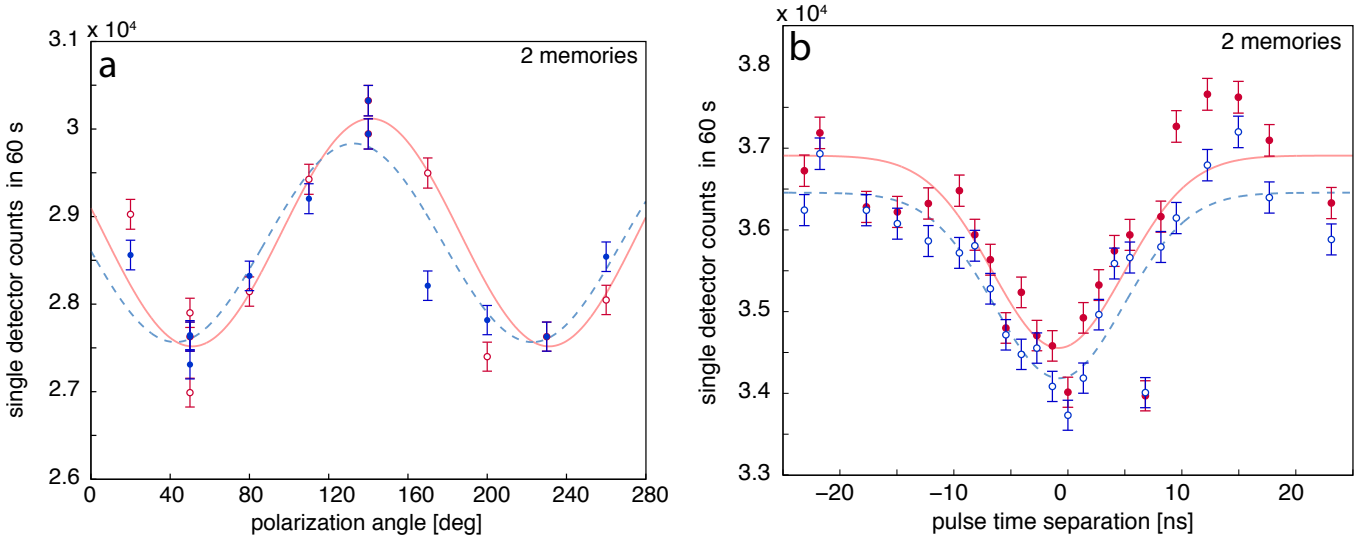


FIG. A3.8: HOM interference manifested in single-detector counts in the case of two active quantum memories when changing a) polarization and b) time difference between pulses at BS input. For the polarization scan in a) we find $\mathcal{V}_{1x} = (8.64 \pm 2.50)\%$ and $\mathcal{V}_{1x} = (7.60 \pm 2.36)\%$ for Si-APD 1 and 2, respectively. For the time scan in b) we measure $\mathcal{V}_{1x} = (6.38 \pm 2.01)\%$ and $\mathcal{V}_{1x} = (6.23 \pm 1.61)\%$ for Si-APD 1 and 2, respectively.

H. Bell-state measurement.

In this section we derive an analytical expression for the coincidence count rates corresponding to projections onto the $|\psi^-\rangle$ Bell state for time-bin qubits detected by the two detectors at the output of the HOM-BS. To that end, we will introduce a number of approximations as we did previously in order to calculate the HOM interference in the coincidence counts. In the limit of low mean photon numbers, two coherent states impinging onto the two inputs of

a 50:50 BS can be represented in terms of Fock states as

$$
\begin{aligned}
|\psi\rangle_{ab} &= \sqrt{p(1,1)}|11\rangle_{a,b} + \sqrt{p(2,0)}|20\rangle_{a,b} + \sqrt{p(0,2)}|02\rangle_{a,b} \\
&= \left(\sqrt{p(1,1)}(\hat{a}^\dagger \otimes \hat{b}^\dagger) + \frac{1}{\sqrt{2!}}\left[\sqrt{p(2,0)}((\hat{a}^\dagger)^2 \otimes I) + \sqrt{p(0,2)}(I \otimes (\hat{b}^\dagger)^2)\right]\right)|00\rangle_{a,b} \quad ,
\end{aligned} \tag{15}
$$

where the subscripts on the state vector refer to the order of listing the input modes, i.e. $|00\rangle_{a,b} \equiv |0\rangle_a \otimes |0\rangle_b$. The factors written as $p(n,m)$ denote the probability of having n and m photons in mode a and b, and are given by $p(n,m) = |({}_a\langle n| \otimes_b \langle m|)(|\alpha\rangle_a \otimes |\beta\rangle_b)|^2 = \frac{e^{-(|\alpha|^2+|\beta|^2)}}{n!m!}(|\alpha|^2)^n(|\beta|^2)^m$. Stemming from the low mean photon number assumption, we do not include terms with more than two photons. Assuming that our detectors are noiseless, terms with a total of one or no photons are also left out as they cannot generate any coincidence counts.

For a time-bin qubit, the Fock state is created in a superposition of two temporal modes, i.e., an *early* (e) and a *late* (l) mode, by the creation operators for the spatial input mode $x^\dagger$ ($x^\dagger = a^\dagger, b^\dagger$) of the beam-splitter, as

$$
(\hat{x}^\dagger)^n|0\rangle_x \rightarrow \left[\cos\Big(\frac{\theta_x}{2}\Big)\ \hat{x}_e^\dagger \otimes I + e^{i\phi_x}\sin\Big(\frac{\theta_x}{2}\Big)\ I \otimes \hat{x}_l^\dagger\right]^n |00\rangle_{xe,xl} \quad , \tag{16}
$$

where $\cos\big(\frac{\theta_x}{2}\big)$ and $\sin\big(\frac{\theta_x}{2}\big)$ are the amplitudes of, and ϕ_x is the relative phase between, the two temporal modes composing the time-bin qubit. The subsript xe refers to the early time-bin of the spatial mode x and similarly for xl. Note, that we sometimes simplify the notation for the time-bin qubit states as $|e\rangle_x \equiv |10\rangle_{xe,xl} = (\hat{x}_e^\dagger \otimes I)|00\rangle_{xe,xl}$. If we insert the expression in Eq. (16) in place of the $\hat{a}$ and $\hat{b}$ operators in Eq. (15) we get the expression for the wavefunction $|\psi(\theta_a,\phi_a,\theta_b,\phi_b)\rangle_{ab}$ for time-bin qubits at the HOM-BS inputs. We split this expression into the various contributions given in Eq. (15)

$$
\begin{aligned}
(\hat{a}^\dagger \otimes \hat{b}^\dagger)|00\rangle_{ab} \rightarrow \frac{1}{2}\Bigg[& \left(ie^{i\phi_b}\cos\Big(\frac{\theta_a}{2}\Big)\sin\Big(\frac{\theta_b}{2}\Big) + ie^{i\phi_a}\sin\Big(\frac{\theta_a}{2}\Big)\cos\Big(\frac{\theta_b}{2}\Big)\right)\left(\hat{c}_e^\dagger\hat{c}_l^\dagger + \hat{d}_e^\dagger\hat{d}_l^\dagger\right) \\
& + \left(e^{i\phi_b}\cos\Big(\frac{\theta_a}{2}\Big)\sin\Big(\frac{\theta_b}{2}\Big) - e^{i\phi_a}\sin\Big(\frac{\theta_a}{2}\Big)\cos\Big(\frac{\theta_b}{2}\Big)\right)\left(\hat{c}_e^\dagger\hat{d}_l^\dagger - \hat{c}_e^\dagger\hat{d}_l^\dagger\right) \\
& + ie^{i(\phi_a+\phi_b)}\sin\Big(\frac{\theta_a}{2}\Big)\sin\Big(\frac{\theta_b}{2}\Big)\left((\hat{c}_l^\dagger)^2 + (\hat{d}_l^\dagger)^2\right) \\
& + i\cos\Big(\frac{\theta_a}{2}\Big)\cos\Big(\frac{\theta_b}{2}\Big)\left((\hat{c}_e^\dagger)^2 + (\hat{d}_e^\dagger)^2\right)\Bigg]|0000\rangle_{ce,cl,de,dl}
\end{aligned} \tag{17a}
$$

$$
\begin{aligned}
((\hat{a}^\dagger)^2 \otimes I)|00\rangle_{ab} \rightarrow \frac{1}{2}\Bigg[& 2e^{i\phi_a}\cos\Big(\frac{\theta_a}{2}\Big)\sin\Big(\frac{\theta_a}{2}\Big)\left(\hat{c}_e^\dagger\hat{c}_l^\dagger - \hat{d}_e^\dagger\hat{d}_l^\dagger\right) \\
& + i2e^{i\phi_a}\cos\Big(\frac{\theta_a}{2}\Big)\sin\Big(\frac{\theta_a}{2}\Big)\left(\hat{c}_e^\dagger\hat{d}_l^\dagger + \hat{c}_l^\dagger\hat{d}_e^\dagger\right) \\
& + \cos^2\Big(\frac{\theta_a}{2}\Big)\left((\hat{c}_e^\dagger)^2 + i2\hat{c}_e^\dagger\hat{d}_e^\dagger - (\hat{d}_e^\dagger)^2\right) \\
& + e^{i2\phi_a}\sin^2\Big(\frac{\theta_a}{2}\Big)\left((\hat{c}_l^\dagger)^2 + i2\hat{c}_l^\dagger\hat{d}_l^\dagger - (\hat{d}_l^\dagger)^2\right)\Bigg]|0000\rangle_{ce,cl,de,dl}
\end{aligned} \tag{17b}
$$

and similarly for $(I \otimes (\hat{b}^\dagger)^2)|00\rangle_{ab}$. Again, the subscripts on the state vector refer to the order of listing the temporal and spatial modes, e.g. ce labels the early bin of the spatial output mode c.

We will look for coincidence detection events that correspond to projections onto the Bell state $|\psi_-\rangle_{cd} = \frac{1}{\sqrt{2}}(\hat{c}_e^\dagger\hat{d}_l^\dagger - \hat{c}_l^\dagger\hat{d}_e^\dagger)|0000\rangle_{ce,cl,de,dl}$. Such projections correspond to a detection event in the early time-bin in one detector followed by a detection event in the late time-bin in the other detector. This projection occurs with a probability $\mathcal{P}_-(\theta_a,\phi_a,\theta_b,\phi_b) = |\ {}_{cd}\langle\psi_-|\psi(\theta_a,\phi_a,\theta_b,\phi_b)\rangle_{cd}|^2$, which can be computed by combining Eq. (17) with Eq. (15). Assuming equal mean photon numbers at the two inputs $|\alpha|^2 = |\beta|^2 \equiv \mu$ and averaging over the coherent state phases, i.e. the complex angle between α and β, we get the expression

$$
\begin{aligned}
\mathcal{P}_-(\theta_a,\phi_a,\theta_b,\phi_b) \propto \frac{\mu^2 e^{-2\mu}}{8}\Bigg[& 4\sin^2\left(\frac{\theta_a+\theta_b}{2}\right) + \sin^2\big(\theta_a\big) + \sin^2\big(\theta_b\big) \\
& - 2\sin\big(\theta_a\big)\sin\big(\theta_b\big)\Big(1 + \cos\big(\phi_a - \phi_b\big)\Big)\Bigg] \ .
\end{aligned} \tag{18}
$$

With this we are able to calculate the probabilities of projection onto $|\psi^-\rangle$ for different combinations of qubits at the two BS inputs, i.e. for different choices of the angles θ_x and ϕ_x. In turn, this allows us to calculate the $|\psi^-\rangle$ Bell-state measurement error rate as

$$e \equiv \frac{\mathcal{P}_-^{\parallel}}{\mathcal{P}_-^{\parallel} + \mathcal{P}_-^{\perp}}\,, \tag{19}$$

where $\mathcal{P}_-^{\parallel}$ is the projection probability when the two input qubit states are identical, i.e. $\phi_a = \phi_b$ and $\theta_a = \theta_b$, while $\mathcal{P}_-^{\perp}$ is the projection probability for two orthogonal input qubit states. This is also defined in terms of count rates in Eq. (1) in the main text. We will now treat a number of relevant cases.

Expected and observed error rates in the case of $\phi_a = \phi_b = 0$. Using the simplified notation this corresponds to the case were the input qubit states are of the form $|\psi\rangle = \cos\left(\frac{\theta_x}{2}\right)|e\rangle + \sin\left(\frac{\theta_x}{2}\right)|l\rangle$. When depicted on the Bloch sphere these qubits span the xz-plane. Using Eq. (18) we compute the projection probability as

$$\mathcal{P}_-(\theta_a, 0, \theta_b, 0) \propto \frac{\mu^2 e^{-2\mu}}{8}\left[4\sin^2\left(\frac{\theta_a+\theta_b}{2}\right) + \sin^2\big(\theta_a\big) + \sin^2\big(\theta_b\big) - 4\sin\big(\theta_a\big)\sin\big(\theta_b\big)\right]. \tag{20}$$

We are interested in the probability $\mathcal{P}_-^{\parallel}$ for the case in which the input qubits are parallel ($\theta_a = \theta_b$) and $\mathcal{P}_-^{\perp}$ for the case in which the input qubit states are orthogonal ($\theta_a = \theta_b - \pi$). Specifically, when we prepare two qubits (one at each input of the BS) in state $|e\rangle$, or two qubits in state $|l\rangle$, we expect $\mathcal{P}_-^{\parallel} = 0$. The probability for observing a projection onto $|\psi\rangle$ increases as we change θ_a (or θ_b), and reaches a maximum $\mathcal{P}_-^{\perp}$ if one qubit is in state $|e\rangle$ and the other one in $|l\rangle$. Hence, using the expression for the error rate above (Eq. (19)), we find $e_{e/l}^{(\mathrm{att})} = 0$.

We now turn to measuring the coincidence rates for all combinations of $|e\rangle$ and $|l\rangle$ input states, and thus extracting $\mathcal{P}_-^{\parallel}$ and $\mathcal{P}_-^{\perp}$, using 0.6 photons per qubit at the memory input. More precisely, we prepare the input qubit state $|e\rangle_a \otimes |e\rangle_b$ to measure $\mathcal{P}_-^{\parallel(1)}$ and then $|e\rangle_a \otimes |l\rangle_b$ to measure $\mathcal{P}_-^{\perp(1)}$. Subsequently, we prepare the input qubit state $|l\rangle_a \otimes |l\rangle_b$ to measure $\mathcal{P}_-^{\parallel(2)}$ and then $|l\rangle_a \otimes |e\rangle_b$ to measure $\mathcal{P}_-^{\perp(2)}$. These yield the average values $\mathcal{P}_-^{\parallel} = (\mathcal{P}_-^{\parallel(1)} + \mathcal{P}_-^{\parallel(2)})/2$ and $\mathcal{P}_-^{\perp} = (\mathcal{P}_-^{\perp(1)} + \mathcal{P}_-^{\perp(2)})/2$, from which we compute the experimental error rate $e_{e/l}^{(\mathrm{exp})} = 0.039 \pm 0.037$, which is near the theoretical lowest value of $e_{e/l}^{(\mathrm{att})} = 0$.

Expected and observed error rates in the case of $\theta_a = \theta_b = \pi/2$. In this case the two input qubits are in equal superpositions of early and late bins, that is of the form $|\psi\rangle = \frac{1}{\sqrt{2}}\big(|e\rangle + e^{i\phi_x}|l\rangle\big)$. On the Bloch sphere these are qubits that lie in the xy-plane. In this case we compute

$$\mathcal{P}_-(\pi/2, \phi_a, \pi/2, \phi_b) \propto \frac{\mu^2 e^{-2\mu}}{4}\big(2 - \cos(\phi_a - \phi_b)\big)\,, \tag{21}$$

Thus the $|\psi^-\rangle$ Bell-state projection probability is smallest – but nonzero – when $\phi_a - \phi_b = 0$, i.e. the qubit states are parallel, and largest when the phases differ by π, i.e. the qubit states are orthogonal. Inserting these values for $\mathcal{P}_-^{\parallel}$ and $\mathcal{P}_-^{\perp}$ into Eq. (19) results in an expected error rate of $e_{+/-}^{(\mathrm{att})} = 0.25$.

Using again 0.6 photons per qubit, we measure the coincidence counts for $\phi_a - \phi_b = 0$ and π giving us $P_-^{\parallel}$ and $P_-^{\perp}$, respectively. From these we get an error rate of $e_{+/-}^{(\mathrm{exp})} = 0.287 \pm 0.020$, which is slightly above the theoretical bound. This indicates that either the measurement suffers from imperfections such as detector noise or the modes at the BS are not completely indistinguishable, which in turn could be due imperfectly generated qubit states or imperfect storage of the qubit in the quantum memory. To be conservative in our assessment of our quantum memory we assume that the entire increase of the measured values of $e^{(\mathrm{exp})}$ is due to the memory fidelity being less than one.

Bounds for attenuated laser pulses stored in quantum and classical memories: We now compare the performance of our Bell-state measurement to a number of relevant bounds assuming always that any imperfections arise from the imperfect storage of the photon in the memory. We will derive bounds to the error rate in the case of one qubit being stored in either a classical memory (CM) or quantum memory (QM). To accommodate this scenario we assume that the memory performs the following operation $|\psi\rangle\langle\psi| \to F|\psi\rangle\langle\psi| + (1-F)|\psi^\perp\rangle\langle\psi^\perp|$, where F denotes the fidelity of the stored state and $|\psi^\perp\rangle$ is the state orthogonal to $|\psi\rangle$. For a classical memory $F^{\mathrm{CM}} = 0.667$ [6] whereas for a quantum memory $F^{\mathrm{QM}} = 1$.

Doing the replacement $\mathcal{P}_-^{\parallel} \to F\mathcal{P}_-^{\parallel} + (1-F)\mathcal{P}_-^{\perp}$ and likewise for $\mathcal{P}_-^{\perp}$ we can express the error rate expected after

imperfect storage of one of the pulses partaking in the Bell-state measurement:

$$e = \frac{F\mathcal{P}_-^{\parallel} + (1-F)\mathcal{P}_-^{\perp}}{\mathcal{P}_-^{\parallel} + \mathcal{P}_-^{\perp}}\,, \tag{22}$$

where in this case the probabilities $\mathcal{P}_-^{\parallel}$ and $\mathcal{P}_-^{\perp}$ refer to those expected without the memory. Since the expected values for $\mathcal{P}_-^{\parallel}$ and $\mathcal{P}_-^{\perp}$ differ between the e/l and $+/-$ bases we treat them separately.

Beginning with the e/l basis we use Eq. (22) with the values from Eq. (20) to derive a bound for the error rate of the Bell-state measurement for one of the two qubits being recalled from a quantum or a classical memory. We find that $e_{e/l}^{(\mathrm{att})} = 1 - F$, and hence we establish the two bounds $e_{e/l}^{(\mathrm{att,QM})} = 0$ and $e_{e/l}^{(\mathrm{att,CM})} = 0.333$. This clearly shows that a classical memory would cause a larger error rate than the $e_{e/l}^{(\mathrm{exp})} = 0.039 \pm 0.037$ measured after storage in our memory. We can also reverse the equations and estimate our memory's fidelity based on the measured error rate. In this case, inserting $e_{e/l}^{(\mathrm{exp})}$ into Eq. (22), we deduce the value $F_{e/l}^{\mathrm{exp}} = 0.961 \pm 0.037$.

We now turn to the $+/-$ basis. For attenuated laser pulses we insert into Eq. (22) the values $\mathcal{P}_-^{\parallel} = 1/4$ and $\mathcal{P}_-^{\perp} = 3/4$ computed from Eq. (21), which enables us to relate the error rate to the memory fidelity as $e_{+/-} = (3-2F)/4$. Thus, one obtains the theoretical lower bound on the error rate $e_{+/-}^{(\mathrm{att,QM})} = 0.250$ for an ideal quantum memory ($F^{\mathrm{QM}} = 1$) and $e_{+/-}^{(\mathrm{att,CM})} = 0.417$ with an optimal classical storage device ($F^{\mathrm{CM}} = 2/3$). We make the observation that our experimental error rate $e_{+/-}^{(\mathrm{exp})} = 0.287 \pm 0.020$ is much below the bound for a classical memory. Based on the experimental error rate $e_{+/-}^{(\mathrm{exp})} = 0.287 \pm 0.020$ we derive an experimental value for the memory fidelity of $F_{+/-}^{\mathrm{exp}} = 0.926 \pm 0.041$. The estimates of the memory fidelity $F_{e/l}^{\mathrm{exp}}$ and $F_{+/-}^{\mathrm{exp}}$ derived from our measurements in two bases are equal to within the experimental error. This together with the fact that their values are well above 0.667 reaffirms our claim that our storage device outperforms a classical memory.

We emphasize once more that we have assumed that the reduction in error rates is due solely to the memory and thus indicates the fidelity of the memory. However, this is likely not the case as imperfections in the state preparation and detector noise also contribute to the reduction in error rate.

Bounds for single photons stored in quantum and classical memories: Although we do not use single photon sources for the experiments reported here, it is interesting to determine how well our results measure up to those that could have been obtained if single photon sources had been employed. In the following we will derive the error rate for the Bell-state measurement using qubits encoded into single photons. To this end we step back to Eq. (15), and note that for single photon sources all probabilities are 0 except for $p(1,1)$, which describes the probability of having a single photon at each BS input. Thus, in the output state we only need to keep the terms from Eq. (17a), which in turn means that the Bell-state projection probability can be written as

$$P_-(\theta_a, \phi_a, \theta_b, \phi_b) \propto \frac{1}{4}\left[\sin^2\left(\frac{\theta_a + \theta_b}{2}\right) + \sin^2\left(\frac{\theta_a - \theta_b}{2}\right) - \sin\big(\theta_a\big)\sin\big(\theta_b\big)\cos\big(\phi_a - \phi_b\big)\right]. \tag{23}$$

It is easily seen that for any two parallel input qubit states ($\theta_a = \theta_b$ and $\phi_a = \phi_b$) we get $P_-^{\parallel} = 0$. Therefore, irrespective of the projection probability for orthogonal input qubit states the expected error rate is always $e^{(\mathrm{sing})} = 0$, where *sing* identifies this value as belonging to the single photon case.

Gauging the effect of storing one of the single photons partaking in the Bell-state measurement in a memory is thus independent of the basis and using Eq. (22) we derive $e^{(\mathrm{sing,QM})} = 1 - F^{\mathrm{QM}} = 0$ and $e^{(\mathrm{sing,CM})} = 0.333$. Contrasting the error rate expected for a photon stored in a classical memory with the two values $e_{e/l}^{(\mathrm{exp})} = 0.039 \pm 0.037$ and $e_{+/-}^{(\mathrm{exp})} = 0.287 \pm 0.020$ obtained experimentally, we recognize that both are well below $e^{(\mathrm{sing,CM})}$. This means that even with a single photon source at ones disposal the error rates that we measured could not have been attained with a classical memory.

Experiments at mean photon numbers above one. In this final section we will explore in greater detail the HOM interference dependence on the angle $\phi_a - \phi_b$ between a set of equal superposition qubit states $|\psi\rangle_x = \frac{1}{\sqrt{2}}\big(|e\rangle + e^{i\phi_x}|l\rangle\big)$, which in line with the preceding sections belong to the $+/-$ basis. According to Eq. (21) the coincidence count rates vary as function of $\cos\big(\phi_a - \phi_b\big)$. In Fig. A3.9 we show measured coincidence count rates as function of $\phi_a - \phi_b$ for a mean photon number per qubit before the memory of around 20. As expected the coincidence detection probability reaches its maximum $\mathcal{P}_-^{\perp}$ when two input qubits are orthogonal ($\phi_a - \phi_b = \pi$) and when they are identical ($\phi_a - \phi_b = 0$)

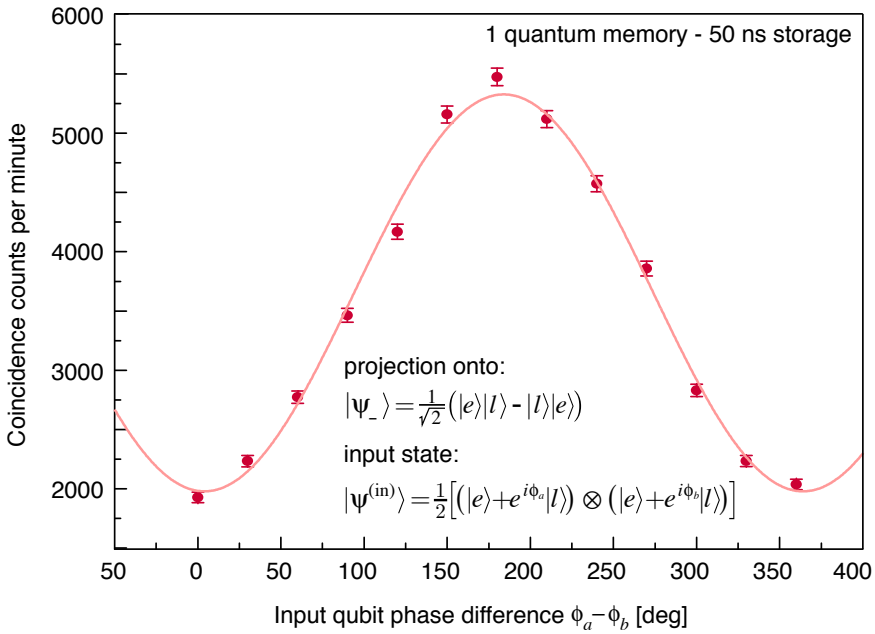


FIG. A3.9: Rate of projection of pairs of time-bin qubits with relative phase $\phi_a - \phi_b$ onto $|\psi^-\rangle$. Each data point was acquired over 60 s

it reaches a minimum $\mathcal{P}_-^{\parallel}$. It is natural to define a Bell-state measurement visibility as

$$\mathcal{V} = \frac{\mathcal{P}_-^{\perp} - \mathcal{P}_-^{\parallel}}{\mathcal{P}_-^{\perp}} \tag{24}$$

analogous to Eq. (1) in the main text. Using values obtained from a cosine fit to the data in Fig. A3.9 yeilds $\mathcal{V}_{+/-}^{\rm exp} = (62.9 \pm 5.2)\%$. Comparing Eq. (24) with Eq. (19) it is easily seen that $\mathcal{V}$ and e are related as $e = (1 - \mathcal{V}_{+/-})/(2 - \mathcal{V}_{+/-})$. We can then use the expected error rates to find the corresponding Bell-state measurement visibilities. Using $e_{+/-}^{att} = 0.25$ we get a theoretical value $\mathcal{V}_{+/-}^{\rm att} = 66.7\%$. In conclusion, our experimental Bell-state measurement visibility is only slightly below and within the experimental error actually equal to the expected value.

[1] Sinclair, N. *et al.* Spectroscopic investigations of a ti:tm:linbo3 waveguide for photon-echo quantum memory. *Journal of Luminescence* **130**, 1586 – 1593 (2010).

[2] Chaneliere, T. *et al.* Storage and retrieval of single photons transmitted between remote quantum memories. *Nature* **438**, 833–836 (2005).

[3] Eisaman, M. D. *et al.* Electromagnetically induced transparency with tunable single-photon pulses. *Nature* **438**, 837–841 (2005).

[4] Moiseev, S. A. & Arslanov, N. M. Efficiency and fidelity of photon-echo quantum memory in an atomic system with longitudinal inhomogeneous broadening. *Phys. Rev. A* **78**, 023803 (2008).

[5] Rarity, J. G., Tapster, P. R. & Loudon, R. Non-classical interference between independent sources. *Journal of Optics B: Quantum and Semiclassical Optics* **7**, S171 (2005).

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

Supplemental Material: Broadband Waveguide Quantum Memory for Entangled Photons

Erhan Saglamyurek,[1] Neil Sinclair,[1] Jeongwan Jin,[1] Joshua A. Slater,[1] Daniel Oblak,[1]
Félix Bussières,[1,*] Mathew George,[2] Raimund Ricken,[2] Wolfgang Sohler,[2] and Wolfgang Tittel[1]

[1]*Institute for Quantum Information Science, and Department of Physics & Astronomy, University of Calgary, 2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada*
[2]*Department of Physics - Applied Physics, University of Paderborn, Warburger Str. 100, 33095 Paderborn, Germany*

I. PREPARATION OF THE ATOMIC FREQUENCY COMB (AFC)

The AFC amounts to a periodic modulation in frequency of the optical density of the inhomogeneously broadened $^3H_6 \leftrightarrow ^3H_4$ thulium absorption line. It can be generated by optically pumping atoms to off-resonant shelving levels - in our case nuclear Zeeman levels [27,31]. To that end, we modulate the intensity of the 795 nm memory laser while scanning its frequency [32]. The frequency sweep is implemented using a lithium niobate phase modulator driven by a 20 GS/s arbitrary waveform generator. To avoid overlap of first and higher order modulation, the sweep extends from 5 GHz to 10 GHz, thus efficiently preparing a 5 GHz-bandwidth AFC memory. The laser intensity modulation is achieved by beating two frequency components, generated in an acousto-optic modulator (AOM) placed before the phase-modulator.

The memory storage time T_s is set by the frequency spacing between the teeth of the AFC, and is determined by $T_s = \delta/\alpha$, where $\delta = 0.35$ MHz is the difference between the two frequency components and $\alpha = 50 \times 10^{12}$ MHz/s is the sweep rate. This yields 142.85 MHz spacing between the AFC teeth, which translates into 7 ns memory storage time. For a high contrast AFC, the chirp cycle is repeated 100 times leading to a 10 ms overall optical pumping duration. The 2.2 ms wait time following the preparation corresponds to 27 times the radiative lifetime of the $^3H_4$ excited level, and ensures no fluorescence masks the retrieved photons.

The optical pumping involves population transfer between ground-state sublevels. As the comb structure extends over all these levels, we carefully chose the magnetic field to make sure that those ions that initially absorb at frequencies where we desire a trough are transferred to frequencies where we desire a peak.

II. THE MEASUREMENT

First, we stabilize the pump interferometer and the 1532 nm interferometer to arbitrarily chosen phase values. We define the phase introduced by the pump interferometer to be zero, i.e. we absorb it into the definition of the "early" and "late" qubit states, leading to the maximally entangled state

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|e,e\rangle + |l,l\rangle\right) \tag{1}$$

Furthermore, we define the measurement performed by the 1532 nm qubit analyzer to be $+\sigma_x$. Next, we change the phase of the 795 nm interferometer and maximize the normalized *joint detection probability*

$$P(\boldsymbol{a},\boldsymbol{b}) = \frac{C(\boldsymbol{a},\boldsymbol{b})}{C(\boldsymbol{a},\boldsymbol{b}) + C(\boldsymbol{a},-\boldsymbol{b})} \tag{2}$$

with a fibre delay line in place of the memory. We define this setting to correspond to a projection onto $+\sigma_x$, and we measure $P_{in}(\sigma_x \otimes \sigma_x)$ over 5 minutes. This measurement (without the memory) is taken as being on the state ρ_{in}, i.e. the bi-photon state before storage.

---

*Current address: Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, 1211 Geneva, Switzerland

	$\sigma_x\otimes\sigma_x$	$\sigma_x\otimes\sigma_y$	$\sigma_x\otimes\sigma_z$	$\sigma_x\otimes$-σ_z	$\sigma_y\otimes\sigma_x$	$\sigma_y\otimes\sigma_y$	$\sigma_y\otimes\sigma_z$	$\sigma_y\otimes$-σ_z
P_{in} [%]	90±2	49±1	49±1	51±1	52±1	10±2	51±1	49±1
P_{out} [%]	89±6	49±8	48±4	52±4	49±6	14±5	49±4	51±4
	$\sigma_z\otimes\sigma_x$	$\sigma_z\otimes\sigma_y$	$\sigma_z\otimes\sigma_z$	$\sigma_z\otimes$-σ_z	-$\sigma_z\otimes\sigma_x$	-$\sigma_z\otimes\sigma_y$	-$\sigma_z\otimes\sigma_z$	-$\sigma_z\otimes$-σ_z
P_{in} [%]	46±1	46±1	94.2±0.1	5.8±0.1	46±1	45±1	7.6±0.2	93.0±0.2
P_{out} [%]	51±6	56±6	94±1	6±1	48±5	52±5	6±1	94±1

TABLE A4.1: **Joint-detection probabilities for density matrix reconstruction:** Measured joint-detection probabilities for all projection measurements required to calculate the density matrices for the bi-photon state emitted from the source (P_{in}), and after storage and recall of the 795 nm photon (P_{out}). Uncertainties indicate one-sigma standard deviations based on Poissonian detection statistics.

	$\sigma_y\otimes(\sigma_x+\sigma_y)$	$\sigma_y\otimes(\sigma_x-\sigma_y)$	$\sigma_x\otimes(\sigma_x+\sigma_y)$	$\sigma_x\otimes(\sigma_x-\sigma_y)$
E_{in} [%]	59.7±1.7	-55.4±1.9	52.0±1.5	70.8±1.8
E_{out} [%]	54±3	-64±4	53±3	53±3

TABLE A4.2: **Correlation coefficients for Bell-inequality tests:** Measured correlation coefficients (see Eq. 3) required to test the CHSH Bell inequality. Uncertainties indicate one-sigma standard deviations based on Poissonian detection statistics.

Next, we add the memory and similarly measure $P_{out}(\sigma_x \otimes \sigma_x)$ over approximately 5 hours. When necessary to change the setting of either qubit analyzer to σ_y, we increase the phase difference introduced by the respective interferometer by $\pi/2$. For projection measurements onto σ_z, we use the delay line in the qubit analyzer. Each joint projection measurement is done with and without memory; the results, given in supplementary table A4.1, allow calculating the density matrices ρ_{in} and ρ_{out} describing the photon pair states before and after storage, respectively [28].

To measure the correlation coefficients

$$E(\boldsymbol{a},\boldsymbol{b}) = \frac{C(\boldsymbol{a},\boldsymbol{b}) - C(\boldsymbol{a},-\boldsymbol{b}) - C(-\boldsymbol{a},\boldsymbol{b}) + C(-\boldsymbol{a},-\boldsymbol{b})}{C(\boldsymbol{a},\boldsymbol{b}) + C(\boldsymbol{a},-\boldsymbol{b}) + C(-\boldsymbol{a},\boldsymbol{b}) + C(-\boldsymbol{a},-\boldsymbol{b})} \tag{3}$$

required for testing the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality [33]. we chose, $\boldsymbol{a} = \sigma_x$, $\boldsymbol{a'} = \sigma_y$, $\boldsymbol{b} = \sigma_x + \sigma_y$, and $\boldsymbol{b'} = \sigma_x - \sigma_y$. Projections onto $\sigma_x \pm \sigma_y$ require changing phase differences by $\pm\pi/4$ as compared to those defining projections onto σ_x. For this measurement we added a detector to the second output of the interferometer in the 795 nm qubit analyzer so that C(**a**,**b**), C(**-a**,**b**), C(**a**,**-b**) and C(**-a**,**-b**) could be measured simultaneously. Measurements without memory are done over 15 min, those with memory over 12-15 hours. The resulting correlation coefficients are detailed in supplementary table A4.2. From these we calculate $S_{in} = 2.379 \pm 0.034 > 2$ before storage and $S_{out} = 2.25 \pm 0.06 > 2$ after storage. Both are approximately equal, larger than 2, and hence violate the CHSH Bell inequality, proving again the presence of entanglement and, beyond that, the suitability of the bi-photon states for quantum key distribution [9]. Moreover, the measured S–values are in good agreement with the respective theoretical values of $S_{th} = 2.235 \pm 0.085$ and $S_{th} = 2.2 \pm 0.22$ calculated using the measured density matrix with uncertainties estimated from Monte-Carlo simulations.

III. CALCULATION OF PURITY, ENTANGLEMENT MEASURES [29] AND FIDELITIES

Assuming an arbitrary two-qubit input state ρ, the *concurrence* is defined as $C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}$, where the λ_i's are, in decreasing order, the square roots of the eigenvalues of the matrix $\rho(\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)$ and ρ^* is the element wise complex conjugate of ρ. The *entanglement of formation* is then calculated as

$$E_F(\rho) = H\left(0.5 + 0.5\sqrt{1 - C^2(\rho)}\right) \tag{4}$$

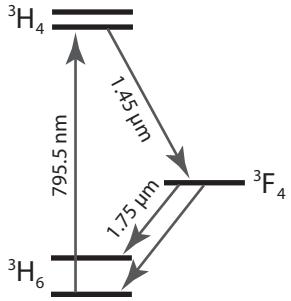


FIG. A4.1: Simplified level diagram for $Tm:LiNbO_3$.

where $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$. Finally, fidelity between ρ and σ is

$$F(\rho,\sigma) = \left(tr\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2 \tag{5}$$

and the *purity* of a state ρ is

$$P = \mathrm{tr}(\rho^2) \tag{6}$$

IV. THE TI:TM:LINBO$_3$ WAVEGUIDE

To fabricate the $Ti:Tm:LiNbO_3$ waveguide, a commercially available 0.5 mm thick Z-cut wafer of undoped, optical grade congruent lithium niobate (CLN) was cut into samples of 12 mm x 30 mm size. Tm doping was achieved by indiffusing a vacuum-deposited (electron-beam evaporated) Tm layer of 19.6 nm thickness. The diffusion was performed at 1130 °C during 150 h in an argon-atmosphere followed by a post treatment in oxygen (1 h) to get a full re-oxidization of the crystal. Tm occupies regular Li-sites when incorporated in CLN by diffusion [34]. The Tm indiffusion leads to a 1/e penetration depth of about 6.5 μm. The maximum Tm concentration of about 1.35×10^{20} cm^{-3} corresponds to a concentration of 0.74 mole %, which is considerably below the solid solubility of Tm in CLN [35]. Subsequently, the waveguide was formed by the well-known Ti–indiffusion technique. At first, a 40 nm thick titanium layer was electron-beam deposited on the Tm-doped surface of the CLN substrate. From this layer, 3.0 μm wide Ti stripes were defined by photo-lithography and chemical etching and subsequently in-diffused at 1060°C for 5 h to form 30 mm long optical strip waveguides. In the wavelength range around 795 nm, the waveguides are single mode for TE- and TM-polarization. To finish the fabrication, the waveguide was cut to 15.7 mm and end faces were carefully polished normal to the waveguide axis.

V. LIMITATION TO EFFICIENCY

While the current system efficiency (characterizing the probability for a photon that enters the cryostat to leave it after recall) of around 0.2% is sufficient to show the entanglement-preserving nature of the storage process, it is clear that this number has to be improved to make the memory more practical and to allow for more involved fundamental measurements.

First, we note that better optical mode matching between the fibre and the $LiNbO_3$ waveguide can be expected to improve the fibre-to-fibre transmission from 10% to 50%.

Second, assuming storage in optical coherence and Gaussian-shaped teeth, the efficiency of the first recall in the forward direction is given by

$$\epsilon = (d_1/F)^2 e^{-d_1/F} e^{-7/F^2} e^{-d_0} \tag{7}$$

where $F = \Delta/\gamma$ denotes the finesse of the comb, and d_1/F and d_0 are the reversible and irreversible optical depth [36] (see supplementary figure A4.1). As discussed above, our comb structure extends over all ground state levels. This fixes the fidelity of the comb to two, as ions can only be "shuffled around" but not removed from the spectral

region covered by the SPDC photons. This impacts on the memory efficiency and sets, according to Eq. 7, an upper bound of $\approx 10\%$. Yet, we note that the memory efficiency can be increased when applying a phase-matching operation that results in backward emission of the stored photon. Further improvement is expected when changing the teeth shape from Gaussian to square [37]. All options combined, it seems possible to achieve a system efficiency of around 15%, which is 75 times larger than in the current implementation. We point out that the limitation due to the comb finesse is not necessarily a consequence of generating broadband combs, but of the small Zeeman splitting of the thulium ground state levels relative to the storage bandwidth. Provided the splitting between the long-lived atomic levels involved in the optical pumping procedure exceeds the storage bandwidth, the finesse can be increased beyond two, and memory efficiencies up to 100% are possible. This may be possible when using the $^3F_4$ level as shelving level, or for other RE impurities featuring greater sensitivity to magnetic fields [38].

VI. LONGER STORAGE TIME AND ON-DEMAND READOUT

Currently, the maximum storage time of our memory is approximately 300 ns. This value is determined by the minimum tooth spacing of the AFC, which is limited by spectral diffusion [27,31]. However, spectroscopic investigation of a Tm:$LiNbO_3$ bulk crystal shows that spectral diffusion decreases when lowering the temperature, similar to the observed improvement of the optical coherence time [31]. This implies the possibility to extend the storage time.

In addition, it may be possible to further improve the storage time and achieve on-demand recall by temporarily transferring the optical excited coherence between the $^3H_6$ and $^3H_4$ levels to coherence between the $^3H_6$ and $^3F_4$ electronic levels, similar to storage of coherence in spin-waves [39]. However, the coherence properties and the suitability of the $^3F_4$ state for such a transfer remains to be investigated. Furthermore, combining the AFC protocol with a quantum memory approach based on controlled reversible inhomogeneous broadening (CRIB) [38] allows one to inhibit the pre-set rephasing of coherence by adding additional, controlled inhomogeneous broadening of each line in the AFC. Rephasing would occur only after reversing, i.e. undoing, the additionally introduced dephasing, and readout would be possible after any multiple of the AFC recall time determined by the tooth spacing.

[30] Thiel, C.W., Sun, Y., Böttger, T., Babbitt, W.R. and Cone, R.L. Optical decoherence and persistent spectral hole burning in Tm^{3+}:$LiNbO_3$. J. Lumin, 130 (9), 1603-1609 (2010).

[31] Reibel R.R., Barber, Z.W., Fischer, J.A., Tian, M. and Babbitt, W.R. Broadband demonstrations of true-time delay using linear sideband chirped programming and optical coherent transients. J. Lumin. 107, 103-113 (2004).

[32] Clauser, J.F., Horne, M.A., Shimony, A. and Holt, R.A. Proposed experiment to test local hidden-variable theories. Phys. Rev. Lett. 23, 880-884 (1969).

[33] Novikov, D. V. et al. Plane wave GID topography of defects in lithium niobate after diffusion doping, Nuclear Instruments and Methods in Physics Research B 97, 342-345 (1995).

[34] Quintanilla, M., Cantelar, E., Sanz-Garca, J.A. Cusso, F. Growth and optical characterization of Tm^{3+}-doped $LiNbO_3$. Optical Materials 30, 1098-1102 (2008).

[35] Afzelius, M., Simon, C., de Riedmatten, H. and Gisin, N. Multimode quantum memory based on atomic frequency combs. Phys. Rev. A 79, 052329 (2009).

[36] Bonarota, M., Ruggiero, J., Le Gouët, J.-L. and Chanelière, T. Efficiency optimization for Atomic Frequency Comb storage. Preprint at http://arxiv.org/abs/0911.4359 (2009).

[37] Tittel, W. et al. Photon-echo quantum memory in solid state systems. Laser and Photon. Rev. 4, (2), 244-267 (2010).

[38] Afzelius, M. et al. Demonstration of Atomic Frequency Comb Memory for Light with Spin-Wave Storage. Phys. Rev. Lett. 104, 040503 (2010).