High-Dimensional Quantum Key Distribution Over Deployed Fiber

by

Catherine Lee

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Electrical Engineering and Computer Science

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

February 2018

Author .....
Department of Electrical Engineering and Computer Science
September 22, 2017

Certified by .....
Dirk R. Englund
Jamieson Career Development Assistant Professor of Electrical Engineering and Computer Science
Thesis Supervisor

Accepted by .....
Leslie A. Kolodziejski
Chairman, Department Committee on Graduate Theses

High-Dimensional Quantum Key Distribution Over Deployed Fiber

by

Catherine Lee

Submitted to the Department of Electrical Engineering and Computer Science
on September 22, 2017, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy in Electrical Engineering and Computer Science

Abstract

Quantum key distribution (QKD) exploits the inherent strangeness of quantum mechanics to improve secure communication, enabling two pre-authenticated participants to establish symmetric encryption keys over long distances, without making any assumptions about the computational abilities of an adversary. QKD commonly relies on the transmission and detection of single photons to distribute the secret keys, but the secret-key generation rates are often limited by hardware, namely the ability to produce or detect nonclassical states of light. We address this challenge by using high-dimensional encoding to increase the secure information yield per detected photon. In this thesis, we present security analysis for and the first demonstrations of a resource-efficient high-dimensional QKD protocol, including two varieties of implementation that each have different strengths and weaknesses. We introduce a 42-km deployed fiber testbed that we use to demonstrate our high-dimensional QKD protocol. We also demonstrate the violation of a steering inequality, confirming that we can produce entanglement in the lab and distribute it over the deployed fiber. By these experiments, we demonstrate both the utility of our high-dimensional QKD protocol and the feasibility of our testbed for further applications in quantum communication and networking.

Thesis Supervisor: Dirk R. Englund
Title: Jamieson Career Development Assistant Professor of Electrical Engineering and Computer Science

Acknowledgments

There are lots of people to thank. I will fill in this section later.

DISTRIBUTION STATEMENT A: Approved for public release: distribution unlimited.

This material is based upon work supported by the Assistant Secretary of Defense for Research and Engineering under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Assistant Secretary of Defense for Research and Engineering.

Parts of this work were also supported by the DARPA Information in a Photon program, through grant W911NF-10-1-0416 from the Army Research Office, and the Columbia Optics and Quantum Electronics IGERT under NSF grant DGE-1069420.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation for quantum key distribution

1.1.1 The quantum menace

As a society, we rely heavily on communication networks: we conduct financial transactions, we transmit personal and/or sensitive information, and we socially interact with other people. We store data on remote cloud servers to retrieve it from any physical location. We conduct searches to access a wide range of information. However, we cannot always control the route our data packets take between source and destination [9, 10]. On untrusted routes, our data is vulnerable to interception by unauthorized agents, and it should not have to be. Encryption is vital for securing our data[1].

To encrypt our communications, most of today's secure internet traffic uses public-key cryptography to authenticate and establish shared session keys between remote entities. However, public-key cryptosystems are not unconditionally secure; their security relies on the difficulty of solving certain mathematical problems and on the assumption that the computational resources needed to solve those problems are unfeasible for an adversary. Three of the most commonly used public-key schemes, Diffie-Hellman (DH) [12], RSA [13], and elliptic curve cryptography (ECC) [14, 15],

[1] And for keeping it private — security $\neq$ privacy, but both are important [11].

underpin most of the cryptography used on the internet today [16]. These cryptosystems all rely on the hardness of integer factorization or computing discrete logarithms. A quantum computer implementing Shor's algorithm [17] could (in theory) break DH, RSA, and ECC easily by finding discrete logarithms and factoring numbers in polynomial time — scaling exponentially better than the current best known classical algorithm, the number field sieve [18, 19].

In light of this quantum threat, Mosca motivates the investigation of quantum-resistant cryptographic solutions by comparing three time intervals [20]:

1. The security shelf-life, or how long the cryptographic keys must remain secure (denoted as x).

2. The migration time, or how long it will take to deploy a set of quantum-safe security tools (denoted as y).

3. The collapse time, or how long it will take for a quantum computer (or something else) to break the currently deployed public-key tools (denoted as z).

If $x + y > z$, the current cryptosystem is vulnerable [20]. Various academics [21], government agencies [22], and international working groups [16] are concerned about mitigating the threat to secure communication posed by quantum computers.

1.1.2 The quantum strikes back

Besides posing a threat to the secure internet as we know it, quantum information processing (QIP) offers a potential solution in the form of quantum key distribution (QKD). QKD enables two pre-authenticated participants, traditionally known as Alice and Bob, to establish secret, identical keys over long distances [23]. The output keys have universally composable security [24], allowing them to be used as inputs to classical encryption schemes such as the one-time pad (OTP) [25].

The OTP is a symmetric encryption scheme that offers information-theoretic security, which does not require assumptions about an adversary's abilities and is therefore not susceptible to any potential speedups provided by a quantum computer. The OTP

requires the two users to hold identical and secret keys. To encrypt, each plaintext bit is combined with a key bit by the exclusive-or (XOR) operation. The resulting ciphertext is decrypted by XOR-ing with the same key. Barring human factors such as theft, loss, improper disposal, or reuse of the key, the OTP is provably (i.e., information-theoretically) secure [26]. However, because the keys must be at least as long as the plaintext, the challenging aspect of the OTP is secure key exchange. Historically, this restricted the use of the OTP to ultra-secure, low-bandwidth channels [27]. QKD aims to solve the key exchange problem by enabling two geographically separated users to establish a symmetric encryption key with security based on the laws of physics.

A special feature of QKD is its ability to provide intrusion detection during the key exchange process. Alice and Bob can detect the interference of an adversary, traditionally known as Eve. Eve's interference can be quantified, and if it is beyond an acceptable threshold, Alice and Bob will abort the protocol rather than use an insecure key [23]. However, a potential drawback of QKD is the requirement that Alice and Bob have previously authenticated themselves to each other [28], which necessitates that they hold a prior shared secret. For this reason, QKD is best understood as a tool to expand a short secret key to a much longer secret key, rather than a tool to generate unconditionally secure keys from scratch [29]. Secure schemes exist to establish authentication using a key much shorter than the messages to be authenticated [30], and therefore, following a precedent set by two of the inventors of QKD [29, 31], our work will assume that Alice and Bob are already authenticated.

However, QKD is not a security panacea: it obviates the mathematical complexity assumptions currently required by common encryption schemes only to replace them with a legion of new assumptions related to physical implementations [32, 33]. Despite these new challenges, QKD is expected to become an increasingly valuable tool for securing communications [34].

1.2 High-dimensional quantum states

1.2.1 High-dimensional quantum information processing

In QKD, Alice sends quantum states to Bob. The quantum states are traditionally carried by so-called flying qubits — photons. A qubit, or quantum bit, is a quantum system that can be in one of two states. For photons, the states can be represented by physical degrees of freedom, including but not limited to polarization, frequency, or spatial mode. The first QKD protocols used qubits based on the polarization states of photons [31, 35, 36].

High-dimensional (or large-alphabet) QIP aims to encode more than one bit of information per photon by using photonic degrees of freedom with dimension $d > 2$. Candidate degrees of freedom for qudits (the d-dimensional equivalent of a qubit) include frequency, time, spatial mode, momentum, or orbital angular momentum (OAM) mode. (Polarization is not a good candidate for qudits, as there are only two orthogonal polarization states; however, it can be combined with other degrees of freedom to produce hyperentangled states [37].)

Compared to qubit states, high-dimensional quantum states can provide practical advantages for QIP in terms of resource usage, or task efficiency. For instance, high-dimensional quantum states make it easier to violate Bell-like inequalities in tests of local realism [38–42]. The state fidelity [40, 43] and detection efficiency [41, 44] required for violation are both lower for qudits compared to qubits. Working with $d > 2$ can also reduce the number of entangled photons required to collectively teleport the state of multiple qubits [45]. Qudit states can also provide some efficiency advantages over classical information processing. Brukner *et al.* proved that every Bell (or high-dimensional Bell-like) inequality is associated with a communication complexity problem, and states that violate the inequality can be used to solve the communication problem more efficiently than any classical protocol could [46, 47].

High-dimensional QIP could also lead to more efficient quantum gates [48] or quantum error correction [49]. Qudit states are also interesting for use in quantum metrology, as they could lead to improved sensitivity; for example, using high-

dimensional OAM states could provide greater sensitivity (compared using to qubit states) in angular resolution [50].

Most relevantly for this work, high-dimensional quantum states can potentially have a large information content per photon [51, 52], and high-dimensional encoding can provide higher resilience to loss and noise in QKD [53–55].

1.2.2 High-dimensional quantum key distribution

In high-dimensional (i.e., large-alphabet) QKD [56], Alice transmits qudits to Bob to establish a key at a potentially higher rate than that afforded by traditional, two-level QKD protocols. Because QKD is primarily motivated by the OTP[2], and because OTP encryption consumes one key bit for each bit of plaintext, key generation rates should ideally approach data communication rates. However, state-of-the-art QKD systems have not yet demonstrated secret-key rates higher than Mbps [3, 59].

The first QKD protocols relied on binary encoding in discrete polarization states [31, 35, 36], which could result in at most one bit of secure information per detected photon. Since single photons of light are difficult to reliably produce and detect, the motivation for large-alphabet QKD is to increase the information per detected photon above the one-bit limit of binary QKD. Instead of polarization, there are a variety of other candidate degrees of freedom. To date, studies of large-alphabet QKD have investigated position-momentum in free-space [60–62], spatial modes in multicore fibers [63, 64], time-energy [2, 4, 52, 65–76], and OAM modes [77–79].

1.2.3 High-dimensional time-energy entanglement

To implement QKD in today's telecommunications infrastructure, time-energy qudits are particularly appealing because they are preserved when transmitted through

[2]The QKD outputs can be used with any symmetric encryption protocol, including block ciphers such as AES. Such schemes are not information-theoretically secure, but quantum computing is expected to provide only a quadratic speedup in cracking block ciphers [57], making their continued use more feasible than encryption schemes that rely on integer factorization or discrete logarithms. Block ciphers benefit from frequent key refreshing, which is challenging classically but can be aided by QKD [23]; indeed, QKD has been demonstrated in conjunction with real-time AES-256 encryption with rekeying [58].

single-mode optical fiber, which is not true for polarization, position-momentum, or OAM modes. The time-energy correlations are also compatible with wavelength division multiplexing (WDM) systems, which can potentially reduce infrastructure requirements by combining several quantum and/or classical signals on the same optical fiber.

Optical fiber has two low-loss spectral windows around 1310 nm and 1550 nm. Advanced time-energy-entangled photon pair sources have been developed for both windows using either spontaneous four-wave mixing [80–83] or spontaneous parametric downconversion (SPDC) [84–86]. In this thesis, we focus on high-dimensional time-energy entanglement produced by SPDC [87]. SPDC is a nonlinear optical process that converts a pump photon into two daughter photons (called signal and idler), while conserving both energy and momentum. The signal and idler photons are correlated in emission time and anticorrelated in frequency. SPDC can produce entangled states with a very large number of dimensions, d, and thus a very high information content, $\log_2 d$ bits, per photon [51, 52].

Time-energy entanglement can be verified using a Franson interferometer [88], which comprises two unbalanced interferometers, one at Alice's location and one at Bob's. The original Franson interferometer setup analyzes only two temporal modes, but by increasing the number of interferometers, multiple temporal modes can be measured [75, 89–91]. An alternative measurement strategy uses interferometers and polarizing beamsplitters to convert timing information to polarization [43, 92]. However, these methods measure discrete temporal modes defined by the interferometer delays, and the setups become more complex as d gets larger.

Compared to these interferometric techniques, quasi-continuous measurements of time and frequency can be simpler to implement, assuming the availability of more specialized hardware with sufficiently high temporal and spectral resolution. The continous degrees of freedom are discretized by the measurement resolution. Using fast single-photon detectors, time can be measured by direct detection, while frequency can be measured by applying a frequency-dependent temporal shift, e.g., using dispersion [2, 73, 93]. Alternatively, frequency can be measured directly using

a spectrometer, and timing information can be converted to frequency by applying a time-dependent frequency shift, e.g., using a time lens [67, 94]. These continuous measurements can access the large information bandwidth of time-energy-entangled photons for QKD and other applications.

1.3 Field demonstrations of quantum key distribution

Two-dimensional QKD protocols have been demonstrated in long-distance testbeds around the world in both atmospheric channels [95–102] and over deployed fibers [7, 58, 103–113]. Many multi-node fiber network testbeds have also been established for binary QKD [103, 106, 108–111], demonstrating long-term, stable operation and integration with software systems that manage and use the output keys.

On the other hand, high-dimensional QKD experiments have generally been limited to in-lab demonstrations [4, 52, 60, 62, 65, 67, 71, 75, 78, 79], although a recent field test combined two polarization modes and two OAM modes to produce four-dimensional states for QKD over an atmospheric channel [114].

1.4 Outline of this thesis

In this thesis, we describe the first lab and field demonstrations of a recently developed high-dimensional QKD protocol based on time-energy entanglement. Our field demonstration is in fact the first field demonstration of any high-dimensional QKD protocol. In Chapter 2, we introduce essential background information on QKD security and provide context for different families of protocols. In particular, we define and compare the entanglement-based (EB) and prepare-and-measure (P&M) implementations of QKD, both of which are investigated in this thesis. In Chapter 3, we introduce our protocol, dispersive-optics QKD (DO-QKD), and also detail its security analysis. The development of DO-QKD and its first security proof were led by Jacob Mower, in collaboration with Zheshen Zhang and Prof. Jeffrey Shapiro. The first

security proof holds in the asymptotic regime, when the output keys are assumed to be infinitely long. This thesis extends the proof to the more realistic regime of finite-length keys. The finite-key security proof for DO-QKD is also contained in Chapter 3. In Chapter 4, we describe the P&M implementation of DO-QKD and also introduce the 42-km deployed-fiber testbed that runs between MIT in Cambridge, MA, and MIT Lincoln Laboratory (LL) in Lexington, MA. All field demonstrations in this thesis occurred in this testbed, in collaboration with the Optical Communications Technology Group at LL. We present both lab and field demonstrations of P&M DO-QKD and discuss the utility of high-dimensional time-energy encoding. In Chapter 5, we present our work on the EB implementation of DO-QKD, including the construction of SPDC sources, an in-lab demonstration in collaboration with the single-photon detector groups from NIST Boulder and NASA's Jet Propulsion Laboratory, and steps toward a field demonstration in the testbed. We also include further discussion of the trade-offs resulting from high-dimensional time-energy encoding. In Chapter 6, we describe a high-dimensional Einstein-Podolsky-Rosen steering experiment that uses the same setup as EB DO-QKD to confirm the presence and successful distribution of entanglement. In Chapter 7, we summarize our contributions and present suggestions for further work.

Chapter 2

General background on quantum key distribution

In this chapter, we describe some relevant background on QKD protocols and their security. This material provides context for later chapters and will be subsequently expanded upon as needed.

2.1 Goals, assumptions, and attack classifications

QKD enables two parties separated at a distance, traditionally called Alice and Bob, to communicate securely with each other without requiring assumptions about the resources available to an adversary, Eve[1]. After the successful implementation of a QKD protocol, Alice and Bob should hold keys that are identical and secret, i.e., known only to them. The most useful figure of merit of a QKD system is the secret-key rate, i.e., the rate in bits per second at which Alice and Bob build up their secret and identical keys. The secret-key rate is affected by all aspects of the physical system, namely the transmitter, the receiver, and the channel, as well as by theoretical factors such as the protocol choice.

Alice and Bob are connected by an insecure quantum channel and a public but

[1]In classical cryptography, Eve is merely an eavesdropper, and a malicious active attacker is called Mallory [27], but in QKD, Mallory's attributes are given to Eve.

authenticated classical channel. Eve is assumed to have full control over the quantum channel, constrained only by the laws of physics, and all loss, noise, and other non-idealities caused by this channel are attributed to Eve. However, Eve can only eavesdrop on messages passed on the classical channel. The authentication of the classical channel prevents Eve from staging a man-in-the-middle attack or otherwise interfering with messages passed on this channel. She cannot alter or block messages sent by Alice or Bob or inject her own messages. Additionally, Alice and Bob assume that Eve cannot access their laboratories; that is, she cannot access their physical setups and measurement settings [23].

Although Eve is, in theory, constrained only by the laws of physics, it is useful to categorize her possible attacks, listed here from weakest to strongest [115]:

1. Individual attacks: Eve can only interact with Alice's transmitted signals one-by-one, and she must make her measurements after Alice and Bob perform sifting but before they begin their classical postprocessing.

2. Collective attacks: Eve can make a joint measurement over all of Alice's transmitted photons, and she can make her measurement after Alice and Bob's classical postprocessing is complete, taking advantage of additional information leaked over the classical channel during postprocessing.

3. Coherent, or general, attacks: Eve can do anything compatible with the laws of physics.

It is proven for some cases that the security bounds against coherent attacks are equivalent to to those for collective attacks [23, 115, 116].

2.2 Outline of a general protocol

All QKD protocols have two main stages: signal exchange and measurement, which occurs over the quantum channel, followed by classical postprocessing, which is accompanied by messages sent over the classical channel.

There are two main categories of QKD implementations that differ in the signal exchange and measurement stage; they are known as the entanglement-based (EB) and prepare-and-measure (P&M) implementations. EB and P&M implementations are mathematically equivalent, making the same security proofs true for both types [23, 36]. In an EB implementation, Alice produces an entangled-photon pair and transmits half of it over the quantum channel to Bob; they subsequently measure their respective halves of the pair to obtain correlated results. In a P&M implementation, Alice prepares quantum states by encoding information in some photonic degree of freedom and transmits the photon over the quantum channel to Bob, who measures it to recover the information that Alice encoded. The classical postprocessing stage is the same for both EB and P&M implementations.

In both implementations, Alice and Bob use (at least) two different, complementary bases for measurement and/or encoding. After the signal exchange and measurement stage is complete, Alice and Bob compare their basis choices (but not their measurement results) for each clock cycle. They discard instances for which they used different bases. The remaining instances are translated into correlated strings of bits (for two-dimensional protocols) or symbols (for high-dimensional protocols) — the raw keys.

Alice and Bob's raw keys are highly likely to contain errors, so to fix this, Alice and Bob run the raw keys through these classical postprocessing steps:

1. Parameter estimation: Alice and Bob publicly compare a subset of their measurement results to estimate relevant parameters of the quantum channel, such as the error rate or detection rates. This subset must be randomly chosen. If the value of any parameter is beyond some previously agreed-upon threshold, Alice and Bob conclude that Eve's interference was too great to result in a secure key, and they abort the protocol.

2. Error reconcilation: Alice and Bob use classical error correction to remove errors from their raw keys. This step involves communication over the authenticated classical channel and will leak information about the reconciled keys to Eve,

even when using one-way communication to minimize the leakage.

3. Privacy amplification: Alice and Bob remove Eve's information about their reconciled keys by using hash functions to distill secret (but shorter) keys [117, 118].

2.3 Comparison of entanglement-based and prepare-and-measure implementations

Although EB and P&M implementations of QKD are mathematically equivalent [36], they are markedly different in setup complexity and utility. Despite significant development of SPDC sources, including efficient sources based on waveguides [84–86, 119], it can be difficult to produce high-quality entangled pairs at high rates. On the other hand, P&M QKD transmitters require no entanglement sources. P&M QKD has been studied using single-photon sources based on quantum dots [120–125] or defect centers in diamond [126], but the most common light source for P&M QKD is an attenuated laser.

In P&M QKD, Alice uses an attenuated laser to produce weak coherent pulses (WCPs). When the phase of each WCP is random, the state ρ of Alice's laser output can be described by a Poissonian mixture of number states with average intensity (photon number per WCP) μ [23]:

$$\rho = \sum_{n=0}^{\infty} P(n,\mu)|n\rangle\langle n|, \tag{2.1}$$

with

$$P(n,\mu) = \frac{e^{-\mu}\mu^n}{n!}. \tag{2.2}$$

For QKD, only pulses with $n = 1$ are desired; $n = 0$ pulses are considered vacuum and make no contribution to the key, and pulses with $n > 1$ are susceptible to the photon-number-splitting (PNS) attack [127, 128]. In a PNS attack, Eve can detect whether a WCP contains $n > 1$ photons and act accordingly: for $n \leq 1$, she simply prevents

the pulse from reaching Bob, while for $n \geq 2$, she splits the pulse. By transmitting at least one photon to Bob while keeping the rest of the pulse for herself, Eve obtains a copy of the quantum state that Alice sent to Bob. Eve can then measure the state without introducing errors that Alice and Bob can detect.

To guard against a PNS attack, Alice can transmit pulses of varying intensities. Alice and Bob then record the received photon statistics separately for each intensity. The fraction of Bob's received signals corresponding to a given intensity should match the fraction of signals that Alice transmitted with that intensity. This strategy is the so-called decoy-state method [129–131]. Without decoy states, Alice would have to keep her average photon number μ very low to reduce the likelihood of transmitting multi-photon pulses. A low value of μ reduces the single-photon transmission rate and, consequently, the secret-key rate: Alice's optimal intensity scales as t and the secret-key rate scales as t^2, where t is the transmission of the quantum channel connecting Alice and Bob. However, by using decoy states, Alice can achieve the same scaling obtained by single-photon sources: the secret-key rate is linear in t [23]. Decoy states allow Alice to maintain the secret-key rates attainable by single-photon sources while using a convenient and potentially low-cost laser.

One appeal of P&M QKD transmitters is that they can be built using commercial, off-the-shelf (COTS) components, such as lasers, modulators, and attenuators. They can also be constructed compactly and in large numbers using photonic integrated circuits [113, 132, 133]. Additionally, since Alice only prepares quantum states but does not detect them, she requires no single-photon detectors, which can be costly and potentially require cumbersome cooling systems. However, Alice does need multiple satisfactory sources of random numbers: one to generate the raw key, one to determine the basis used for each signal, and one to determine the intensity transmitted for each signal.

The most significant advantage of P&M QKD over EB QKD is that P&M transmitters currently operate at significantly higher rates. Current state-of-the-art P&M systems are clocked at or around 1 GHz [3, 59, 134], while bright SPDC sources produce high-quality entangled pairs at low-MHz-class rates [86]. The highest-rate QKD

demonstrations reported to date use P&M systems [3, 59, 76].

Despite the higher secret-key rates achieved by P&M systems, EB QKD is not obsolete, and it has its own advantages. Only EB systems, in combination with the violation of a Bell inequality [40, 135–138], can be used for device-independent (DI) QKD [139–143] — a category of QKD schemes that aims to eliminate the requirement for trust in the physical implementation of a system. There is a disconnect between a theoretical QKD security proof and the physical implementation of a protocol, which can lead to hardware-related vulnerabilities that are not covered by the theory [32, 33]. In addition to DI QKD, another unique application of EB QKD relates to long-distance transmission: only EB QKD is compatible with quantum repeaters [144], which could counter the effects of loss in the quantum channel and connect users separated by ever-greater distances.

2.4 Two protocol families: discrete and continuous variables

EB and P&M refer to two different types of QKD *implementation*. We would also like to compare two different families of QKD *protocols*.

2.4.1 Discrete-variable quantum key distribution

As the name implies, discrete-variable QKD protocols encode information in discrete degrees of freedom of single photons, such as polarization [7, 31, 96] or discrete phases (measured by interferometers with fixed phase differences between the two arms) [59]. In the first QKD protocol, known as BB84 [31], Alice encoded information in discrete polarization states using two complementary bases. In one basis, the so-called rectilinear basis, Alice can produce either an $|H\rangle$ state with horizontal polarization or a $|V\rangle$ state with vertical polarization. In the other basis, the diagonal basis, Alice can produce either a diagonal state $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ or an antidiagonal state $|A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$. Security was initially based on the intuition that if Eve

were to disturb the states transmitted from Alice to Bob, then on average, she would introduce noticeable errors, and meanwhile, the laws of physics prevent Eve from simply copying the state [145].

Over time, these intuitive notions of security became more formalized. Early security proofs were based on entanglement distillation and then also on its correspondence with QKD postprocessing [146–148]. Later proofs are based on information-theoretic techniques that bound the length of the secret key that can be extracted [24, 115, 149, 150]. Discrete-variable protocols such as BB84 are proven secure against coherent (the most general) attacks [115, 150].

Discrete-variable procotols use single-photon detectors and postselect only successful detection events, i.e., if a photon is lost, then it does not contribute to the key. Thus, loss impacts the secret-key rate because it affects the rate of detection events; however, loss does not directly lead to errors in the raw keys.

2.4.2 Continuous-variable quantum key distribution

Continuous-variable (CV) QKD protocols use standard homodyne or heterodyne receivers to detect the modulation of either squeezed or, more commonly, coherent states of light. Depending on the modulation scheme, CV QKD protocols have the potential to extract > 1 bit of information per received signal.

The receivers can be COTS and are generally faster than single-photon detectors. However, instead of postselecting on successful detection events, the receiver makes a measurement at each clock cycle, and losses in the channel contribute to noise at the receiver. Compared to discrete-variable QKD, Alice and Bob might be able to build up their raw key more quickly, but more intensive error reconciliation is required. Additionally, in terms of secret-key rates, CV QKD protocols perform worse at higher loss. The maximum tolerable loss, and thus attainable distance, of CV QKD is currently lower than that of discrete-variable QKD.

It has been shown that Gaussian attacks are optimal for both individual [151] and collective [152, 153] attacks against CV-QKD. Ref. [154] establishes security against coherent attacks for CV protocols that use squeezed states. For CV protocols that use

coherent states, Ref. [155] proves security against collective attacks and can be easily extended to show security against coherent attacks. Quantum de Finetti theorems can reduce coherent attacks to collective attacks [116], but this approach does not scale well outside the asymptotic limit.

2.5 Finite-key security

In the asymptotic limit, the keys are infinitely long, and Alice and Bob have an infinite number of samples with which to estimate the required parameters such as the error rate. This scenario is unattainable, and realistic security must consider the effects of finite-length keys. The most significant modifications to the security proof are due to the effects of statistical fluctations in the parameters to be estimated [156]. Alice and Bob need to optimize over Eve's possible attacks that are compatible with the observed parameter values, i.e., they must use the worst-case parameter values, considering the statistical fluctations.

It can be nontrivial to translate a security proof from the asymptotic limit to the finite-key regime. Initial finite-key security proofs assumed only collective attacks [157, 158]. For some common protocols such as BB84, the collective-attack security proof could be immediately extended to hold against coherent attacks by taking advantage of symmetries in those protocols [157, 159]. For other protocols, such as all CV QKD protocols, it took a few more years to develop techniques for finite-key security proofs against coherent attacks [154, 155].

Chapter 3

Dispersive-optics quantum key distribution: protocol and security, including finite-key security

In this chapter, we introduce and define dispersive-optics QKD (DO-QKD), a new large-alphabet QKD protocol that uses time-energy encoding, and we prove its security against collective attacks in the finite-key regime [72]. We will later use our finite-key security proof to analyze the security of our DO-QKD experiments.

The work on the development of DO-QKD and its asymptotic security proof was led by Jacob Mower [2]; we briefly summarize the asymptotic security in Section 3.2 because it is the essential starting point for the subsequent work.

3.1 Protocol definition

3.1.1 Signal exchange and measurement

Alice holds an SPDC source that produces pairs of time-energy entangled photons. The biphoton state produced by the SPDC source in the vicinity of time $t = 0$ can

be approximated as

$$|\Psi\rangle = (2\pi\sigma_{\rm coh}\sigma_{\rm cor})^{-1/2} \iint dt_A dt_B \exp\left[-\frac{(t_A+t_B)^2}{16\sigma_{\rm coh}^2} - \frac{(t_A-t_B)^2}{4\sigma_{\rm cor}^2}\right] \times \exp\left[-\frac{i\omega_p(t_A+t_B)}{2}\right]|t_A t_B\rangle, \tag{3.1}$$

where $\sigma_{\rm coh}$ is the coherence time of the SPDC pump field, and $\sigma_{\rm cor}$ is the correlation time between photons, which is set by the phase-matching bandwidth of the SPDC source. $|t_A t_B\rangle = \hat{a}_A^\dagger(t_A)\hat{a}_B^\dagger(t_B)|0\rangle$, and $\hat{a}_{A,B}^\dagger(t_j)$ denotes the photon creation operator for Alice or Bob, respectively, at time t_j. The largest possible alphabet size of the protocol is determined by the Schmidt number K, i.e., the number of possible information eigenstates in the system. This is approximately $K \equiv \sigma_{\rm coh}/\sigma_{\rm cor}$ [52, 160]. Time-energy entangled pairs produced by SPDC can easily achieve Schmidt numbers in the thousands; for example, a source with a phase-matching bandwidth ~ 250 GHz [86] pumped by a continuous-wave (cw) laser with $\sigma_{\rm coh} \sim 100$ ns has a Schmidt number $K = 25,000$.

When Alice's SPDC source produces a photon pair, she keeps one photon and sends the other into the quantum channel to Bob. Alice and Bob measure their photons in the conjugate bases of time and frequency (energy). The time basis (TB) corresponds to direct detection of photon arrival time; the frequency basis (FB) is implemented by direct detection after group-velocity dispersion (GVD) is applied to the photon. To Alice measures in the FB, she applies normal GVD to her photon. When Bob measures in the FB, he applies anomalous GVD of magnitude equal to that applied by Alice.

Alice and Bob use oppositely signed GVD because the photons produced by the SPDC are correlated in arrival time but anticorrelated in frequency. If the entangled photons whose state is described by Eq. (3.1) pass through dispersive media, then, in the limit of long coherence time $\sigma_{\rm coh}$, the correlation time $\sigma_{\rm cor}$ becomes

$$\sigma_{\rm cor}'^2 \approx \frac{1}{\sigma_{\rm cor}^2}\left(\sigma_{\rm cor}^4 + (\beta_{2,A}L_A + \beta_{2,B}L_B)^2\right), \tag{3.2}$$

where $\beta_{2,A}$ ($\beta_{2,B}$) is the GVD introduced by Alice (Bob) over length L_A (L_B) [161]. If we define $\beta L \equiv \beta_{2,A}L_A + \beta_{2,B}L_B$, then as βL increases, the temporal correlation between Alice's and Bob's photons degrades. However, $\sigma'_{\text{cor}} = \sigma_{\text{cor}}$ if $\beta_{2,A}L_A = -\beta_{2,B}L_B$. Thus, if Alice and Bob both record photons in the FB, the original correlations between their photons can be recovered [2]. The use of GVD gives the protocol its name, dispersive-optics QKD (DO-QKD).

In the rest of this thesis, we will use the notation

$$D_A \equiv -\frac{2\pi c}{\lambda^2}\beta_{2,A}L_A \tag{3.3}$$

$$D_B \equiv -\frac{2\pi c}{\lambda^2}\beta_{2,B}L_B, \tag{3.4}$$

where λ is the photon wavelength. We will also use D to indicate a quantity of dispersion when not specifically referencing Alice or Bob. The units of D_A, D_B, and D are ps/nm.

A schematic of the DO-QKD protocol, including the SPDC source and the basis measurements, is shown in Fig. 3-1.

3.1.2 Classical postprocessing

After the signal exchange and measurement stage, Alice and Bob sift their time-tagged data into symbols. Each symbol is a temporal frame comprising M slots of duration T_{slot}, where T_{slot} is limited by the timing resolution of the single-photon detectors. The total duration of a symbol is $M \times T_{\text{slot}}$.

Using the authenticated classical channel, Alice and Bob communicate their basis choices and keep only the results from symbols for which they each registered a single detection event while using the same basis. Alice and Bob convert each of these detection events into a $\log_2 M$-bit symbol, based on the temporal position of the event within the frame, i.e., which slot contained the detected photon. The resulting lists of symbols are the raw keys.

Postprocessing converts the raw keys into secure keys that are identical and secret. Alice and Bob first use classical error correction to reconcile the differences

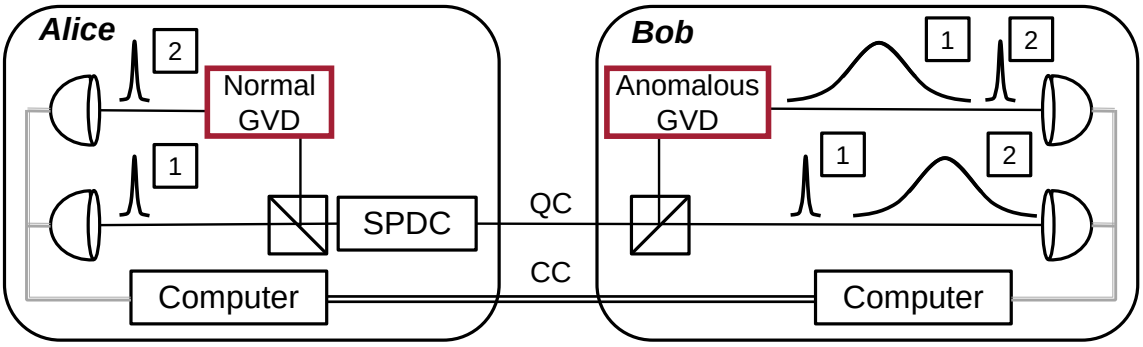

Figure 3-1: Schematic of the DO-QKD procotol. Alice holds the SPDC source. When an entangled photon pair is produced, she keeps one photon and sends the other to Bob using the quantum channel (QC). Alice and Bob have passive splitters that randomly route each photon to one of the two measurements. If Alice measures in the TB (case 1), then Bob's photon is projected into a temporal state. If Bob also measures in the TB, his result is correlated with Alice's; otherwise, the measurement results are uncorrelated. Similarly, if Alice measures in the FB (case 2), then Bob's photon is projected into a frequency state. If Bob also measures in the FB, his result is again correlated with Alice's; otherwise, the measurement results are uncorrelated. Alice and Bob are also linked by an authenticated classical channel (CC) over which they communicate during the classical postprocessing stage.

between their raw keys [1]. The resulting reconciled keys should be identical. Privacy amplification removes information that Eve may hold about the reconciled keys. Privacy amplification is often implemented using 2-universal hash functions. A common method is to multiply the reconciled keys by random Toeplitz matrices [118]. The sifting and postprocessing steps are illustrated in Fig. 3-2.

3.2 Asymptotic security

The following security analysis quantifies the secure information shared using DO-QKD, assuming that Eve can mount arbitrary collective attacks [2, 69] and that the output keys are infinitely long. The analysis combines desirable aspects of discrete-variable and CV QKD protocols. Like discrete-variable QKD, DO-QKD relies on the detection of single photons. Losses reduce the rate of photon detection and thus of key generation but do not add errors to the raw keys. This is preferable to the role that loss plays in CV QKD, in which losses manifest themselves as noise in Bob's

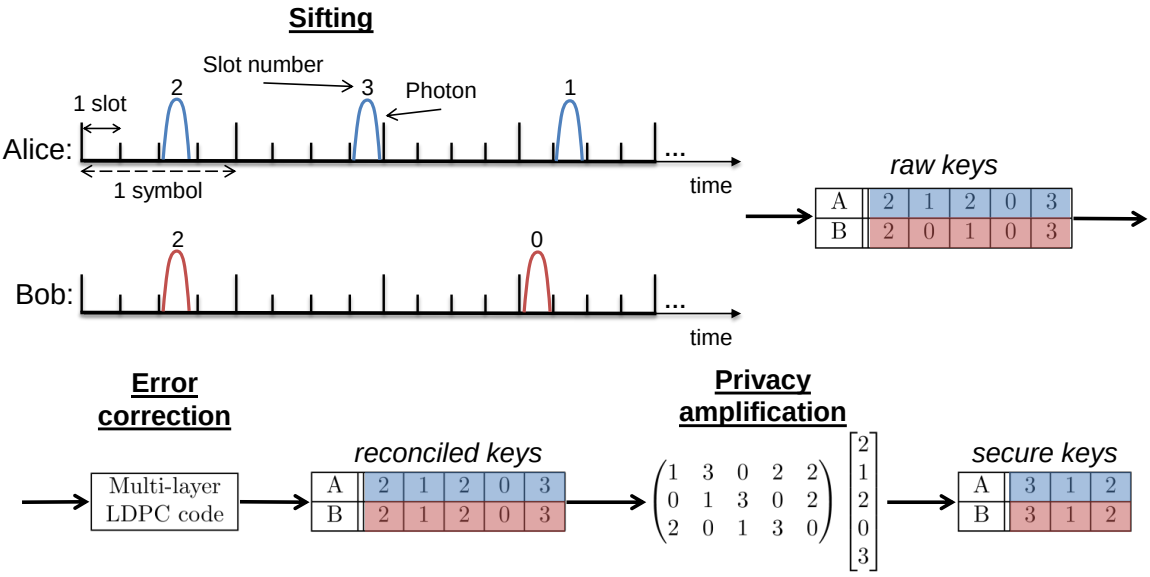

Figure 3-2: Sifting and classical postprocessing, illustrating one measurement basis. A symbol is a temporal frame comprising M slots; in this illustration, $M = 4$. Sifting converts Alice and Bob's measurement results into correlated raw keys with some errors. Error correction is accomplished using a layered low-density parity check (LDPC) code [1] and converts the raw keys to identical reconciled keys. Eve's information about the reconciled keys is eliminated using privacy amplification, leaving Alice and Bob with shorter but secret secure keys.

measurements. However, using CV QKD, it is inherently possible to obtain more than one secure bit per detected signal, while most discrete-variable QKD protocols use binary encoding and are thus limited to one bit. This security proof for DO-QKD adapts the Gaussian-state analysis of CV QKD [162, 163] for single-photon QKD.

The secure photon information efficiency (PIE) quantifies Alice and Bob's information advantage over Eve in units of bits per detected photon coincidence (bpc). In the asymptotic regime, assuming collective attacks, the secure PIE is given by [23, 164]

$$r_\infty = \beta I(A;B) - \chi(A;E), \tag{3.5}$$

where $0 \leq \beta \leq 1$ quantifies the efficiency of the error reconciliation and $I(A;B)$ is Alice and Bob's mutual information, i.e., the information shared after making their correlated photon detection measurements. $\chi(A;E)$ is the Holevo information, i.e., the maximum information that Eve can access about Alice and Bob's measurements, assuming that she is limited to arbitrary collective attacks [152, 153].

An upper bound on $\chi(A;E)$ is computed using the covariance matrix of Alice and Bob's TB and FB measurements. The time-frequency covariance matrix (TFCM) is given by [2]

$$\Gamma = \begin{pmatrix} \gamma_{AA} & (1-\eta)\gamma_{AB} \\ (1-\eta)\gamma_{BA} & (1+\epsilon)\gamma_{BB} \end{pmatrix}, \tag{3.6}$$

where Γ is a four-by-four matrix composed of four two-by-two submatrices. Each submatrix γ_{JK} for $J, K = A, B$ describes the covariance between the measurements of parties J and K. The submatrices are given by

$$\begin{aligned}
\gamma_{AA} &= \begin{pmatrix} \frac{u+v}{16} & -\frac{u+v}{8k} \\ -\frac{u+v}{8k} & \frac{(u+v)(4k^2+uv)}{4k^2uv} \end{pmatrix}, \\
\gamma_{AB} &= \gamma_{BA}^T = \begin{pmatrix} \frac{u-v}{16} & \frac{u-v}{8k} \\ -\frac{u-v}{8k} & -\frac{(u-v)(4k^2+uv)}{4k^2uv} \end{pmatrix}, \\
\gamma_{BB} &= \begin{pmatrix} \frac{u+v}{16} & \frac{u+v}{8k} \\ \frac{u+v}{8k} & \frac{(u+v)(4k^2+uv)}{4k^2uv} \end{pmatrix},
\end{aligned}$$

where $u \equiv 16\sigma_{\text{coh}}^2$, $v \equiv 4\sigma_{\text{cor}}^2$, and $k \equiv 2D$ [2]. In Γ, η represents the decrease in correlations, and ϵ represents the excess noise. These two parameters quantify the effects of Eve's intrustion, channel noise, and setup imperfections.

Instead of directly measuring η and ϵ, it is experimentally easier for Alice and Bob to measure another parameter, ξ, the excess noise factor:

$$\xi \equiv \frac{\sigma^2}{\sigma_0^2} - 1. \tag{3.7}$$

Here, σ^2 is the variance of the measured correlation between Alice and Bob's detected photons, and σ_0^2 is the noiseless variance of that correlation (i.e., excluding Eve's intrusion). Section 3.3.2 will explain that Alice and Bob only need to monitor the excess noise factor in the FB, i.e., the excess spectral noise factor,

$$\xi_\omega = \frac{\sigma_\omega^2}{\sigma_{\omega_0}^2} - 1. \tag{3.8}$$

Here, $\sigma_{\omega_0}^2$ is the noiseless spectral correlation variance, which is determined by the SPDC pump coherence time, σ_{coh}, and the time-bandwidth product. σ_ω^2 is the measured spectral correlation variance between Alice and Bob's detected photons. Because the FB measurement converts frequency information to timing information, σ_ω is in practice derived from σ_t, the two-photon correlation time after Alice and Bob apply equal and opposite GVD of magnitude $|D|$, using the relationship (derived in Appendix A)

$$\sigma_t^2 = \sigma_{\text{cor}}'^2 + |D|^2\sigma_\omega^2, \tag{3.9}$$

where σ'_{cor} is the two-photon correlation time measured in the TB. Thus, the two-photon spectral correlation is given by

$$\sigma_\omega = \frac{\sqrt{\sigma_t^2 - \sigma_{\text{cor}}'^2}}{|D|}. \tag{3.10}$$

Since σ_ω is inversely proportional to $|D|$, the precision of the frequency measurement increases as the dispersion is increased.

The relationship between η, ϵ, and ξ is then given by

$$\epsilon = \frac{-2\eta(K^2 - \frac{1}{4}) + \xi}{K^2 + \frac{1}{4}}, \tag{3.11}$$

where K is the Schmidt number of the SPDC source (which defines the maximum alphabet size). Using their estimate for ξ, Alice and Bob choose values of η and ϵ that maximize the Holevo information while satisfying Eq. (3.11) and the following conditions [2]:

1. Eve cannot increase Alice and Bob's Shannon information by interacting with only Bob's photons, due to the data processing inequality.

2. The symplectic eigenvalues of the covariance matrix are greater than $1/2$, satisfying the Heisenberg uncertainty relation.

3. Eve can only degrade (and not improve) Alice and Bob's measured arrival-time correlation.

The calculation of $\chi(A;E)$ then follows from the symplectic decomposition of the TFCM [2, 69].

3.3 Finite-key security

The security analysis presented thus far holds only in the asymptotic regime, when the output keys are infinitely long. We now amend it to show more realistic security in the finite-key regime. In practice, this amounts to subtracting correction terms from the asymptotic secure PIE defined in Eq. (3.5) and updating the estimate of the Holevo information. When the finite-key corrections are large compared to the asymptotic secure PIE, then no secure key can be obtained.

The most significant cause of finite-key corrections is the statistical fluctuations in the estimated parameters [156]. Finite-key security analysis provides an estimate for the number of signals that Alice and Bob must exchange to estimate the excess spectral noise factor with sufficient accuracy and attain a positive secure PIE.

3.3.1 ε_s and revised secure photon information efficiency

Outside the asymptotic limit, a protocol cannot be completely secure but only ε_s-secure, where ε_s is defined as the probability that the output key K differs from an ideal key [156, 157]:

$$\varepsilon_s = \frac{1}{2}\|\rho_{KE} - \tau_K \otimes \rho_E\|. \tag{3.12}$$

Here, ρ_{KE} is the joint state between K and Eve's system, τ_K is the completely mixed state on K, and ρ_E is the state of Eve's system. Operationally, ε_s is the tolerated failure probability of the entire protocol [156, 157, 165], where failure means that at the conclusion of the protocol and unbeknownst to Alice and Bob, Eve holds information about the output key.

The failure probability ε_s is the sum of the failure probabilities of each stage of the protocol [156–158, 165, 166]:

$$\varepsilon_s = \varepsilon_{PA} + \bar{\varepsilon} + n_{PE}\varepsilon_{PE} + \varepsilon_{EC}. \tag{3.13}$$

Here, ε_{PA} is probability that privacy amplification fails, leaving Eve with some information about Alice and Bob's secure keys. $\bar{\varepsilon}$ is also related to privacy amplification; it is the smoothing parameter for the smooth min-entropy, which characterizes the amount of secure information that can be extracted using privacy amplification when Eve can hold quantum information [157]. ε_{EC} is the probability that error correction fails, leaving Alice and Bob with reconciled keys that are not identical. ε_{PE} is the probability that parameter estimation fails, meaning that the real value of the parameter is outside the desired confidence interval, and n_{PE} is the number of parameters to be estimated. Failure of any stage of the protocol implies that Alice and Bob are unaware that something has gone wrong [158].

The finite-key secure PIE for the DO-QKD protocol can then be written as [72,

157–159, 165–167]:

$$r_N = \frac{n}{N}\left(\beta I(A;B) - \chi_{\varepsilon_{PE}}(A;E) - \frac{1}{n}\log_2\frac{2}{\varepsilon_{EC}} - \frac{2}{n}\log_2\frac{1}{\varepsilon_{PA}} - (2\log_2 M + 3)\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n}}\right). \tag{3.14}$$

Here, the expression $\beta I(A;B) - \chi_{\varepsilon_{PE}}(A;E)$ is nearly identical to the asymptotic secure PIE defined in Eq. (3.5), but the subscript ε_{PE} indicates that the calculation of the Holevo information must now include the finite-key effects on parameter estimation. N is the total number of photon coincidences detected by Alice and Bob, using any combination of basis choices. The quantity $n \equiv p^2 N$ denotes the number of detection events for which Alice and Bob both chose the TB, where p is the probability that the TB is chosen. We assume that Alice and Bob use the same value of p, and we will see that this value need not be $1/2$. Lastly, M is the alphabet size of the protocol.

3.3.2 Asymmetric basis selection

The factor n/N in Eq. (3.14) reflects the fact that not all of Alice and Bob's detection events contribute to key generation. In particular, the sifted keys comprise only detection events for which Alice and Bob both used the same basis. The first QKD protocols [31, 35, 168] assumed that Alice and Bob choose the two measurement bases with equal probabilities, limiting the probability of a same-basis coincidence to at most 50%. It was later suggested that the probability of a same-basis detection could be increased asymptotically to 1 if Alice and Bob choose one measurement basis with a probability $p > 1/2$ [169]. However, Eve can also derive an advantage from this choice: if she knows the preferred basis, then by using only that basis, she can eavesdrop while introducing fewer errors (compared to the case when $p = 1/2$). This gives Eve a better chance of remaining undetected by Alice and Bob. To remove Eve's advantage, Alice and Bob must further modify the protocol: they divide their same-basis detection events according to the measurement basis used, and they estimate parameters separately for each basis. Security is ensured because if Eve chooses to

eavesdrop in the preferred basis, then she introduces more errors in the other basis [169].

Because the insertion loss of the GVD elements reduces the photon detection rate in the FB, the preferred basis for DO-QKD is the TB. By monitoring the excess spectral noise factor ξ_ω, Alice and Bob can bound Eve's information about the TB measurements. We assume that all $m \equiv (1-p)^2 N$ of the FB coincidences are used for parameter estimation to obtain a value for ξ_ω. The value of m is significant because it affects Alice and Bob's ability to estimate ξ_ω with sufficient confidence.

3.3.3 Modified parameter estimation

Alice and Bob have only a finite number of samples with which to estimate ξ_ω, and it is important to know how well their estimate represents the entire dataset. The value of ε_{PE} defines a confidence interval for the estimate of ξ_ω. Within this confidence interval, Alice and Bob must use the worst-case estimate of ξ_ω to upper-bound the Holevo information.

In a sifted symbol-frame, Alice and Bob's detected photon arrival times, T_A and T_B, are jointly-Gaussian random variables. Assuming that the sequence of Alice and Bob's measurements is statistically independent, the estimate for σ_t', the measured two-photon correlation time after applying GVD, denoted $\hat{\sigma}_t'$, has a χ^2 distribution:

$$(m-1)\frac{\hat{\sigma}_t'^2}{\sigma_{\text{cor}}^2} \sim \chi^2(1-\varepsilon_{PE}, m-1). \tag{3.15}$$

According to Eq. (3.10), the necessary estimate of the two-photon spectral correlation, $\hat{\sigma}_\omega'$, is related to $\hat{\sigma}_t'$ by a constant factor, so $\hat{\sigma}_\omega'$ also follows a χ^2 distribution. Then an upper bound on σ_ω' is given by [158]:

$$\sigma_{\omega,\text{UB}}'^2 = \hat{\sigma}_\omega'^2 + \frac{2}{\sqrt{m}}\,\text{erf}^{-1}(1-\varepsilon_{PE})\hat{\sigma}_\omega'^2. \tag{3.16}$$

This bound is valid for the confidence interval $1-\varepsilon_{PE}$. Then, the worst-case estimate

for ξ_ω within the confidence interval is

$$\xi_{\omega,\mathrm{UB}} = \frac{\sigma'^2_{\omega,\mathrm{UB}}}{\sigma^2_{\omega,0}} - 1. \tag{3.17}$$

3.3.4 Numerical results

To ascertain whether DO-QKD can output secure keys in the finite-key regime, we first compute the finite-key secure PIE and plot it for different alphabet sizes $M \in \{8, 16, 32, 64\}$ as a function of N, the number of detected coincidences, in Fig. 3-3, for $\varepsilon_s = 10^{-5}$ [72]. An important figure of merit is the smallest N at which Alice and Bob can obtain a useful amount of secure information. Fig. 3-3 shows that this occurs around $N \approx 10^4$ for the chosen parameter values. This value is comparable to that obtained by traditional, discrete-variable QKD protocols, which are generally able to extract a useful amount of secure information starting at $N \approx 10^5$ [23, 156, 157, 159, 165], and orders of magnitude lower than that of CV QKD protocols, which generally require $N \approx 10^8$ [158, 170].

For all protocols, the inability to obtain secure key at lower N values is due to the finite key length and its effect on Alice and Bob's parameter estimation. Statistical fluctuations in the estimated values have the most deleterious effects on the finite-key secure PIE [156, 159] because Alice and Bob must use the worst-case estimate compatible with ε_{PE} for each parameter. As N gets smaller, the magnitude of the statistical fluctuations increases and the worst-case estimate increasingly deviates from the asymptotic value, lowering the secure PIE.

Fig. 3-4 plots the finite-key secure PIE as a function of channel length for $M = 8$ and different values of $N \in \{10^4, 10^6, 10^8, 10^{10}, \infty\}$ [72]. Besides illustrating the deleterious effects of smaller N on the secure PIE, Fig. 3-4 also confirms that the finite-key secure PIE, just like the asymptotic secure PIE [2], is unaffected by loss. Fig. 3-4 also indicates that even assuming finite-key security, DO-QKD should reach transmission distances > 200 km.

For each value of N, the value of p, the probability of choosing the TB, should be determined numerically to maximize the secure PIE [165]. Fig. 3-5 plots the TB

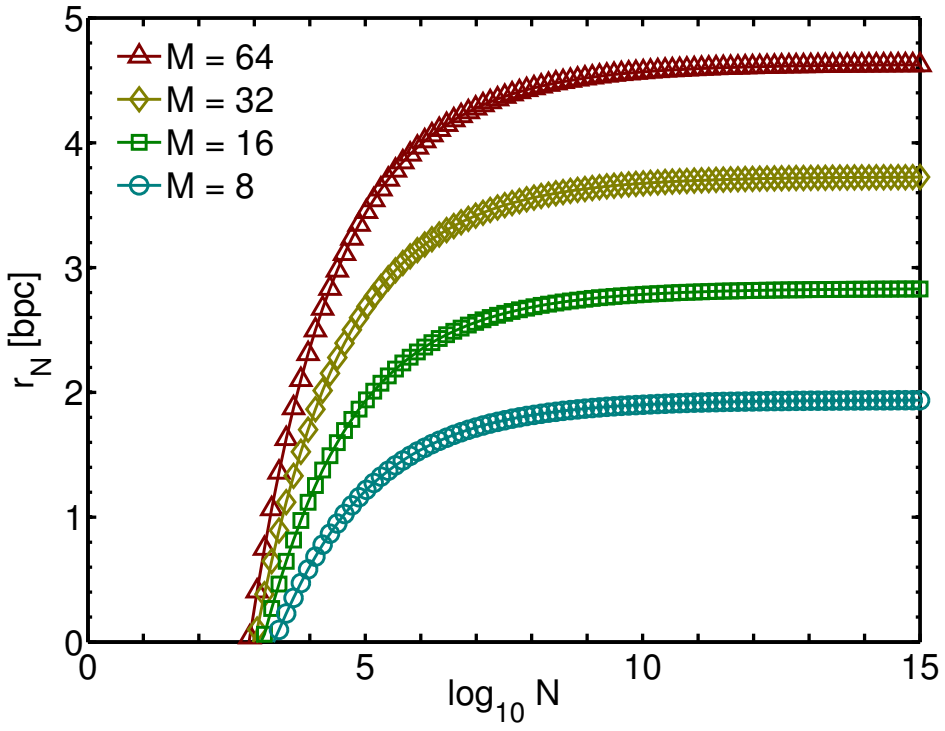

Figure 3-3: Plot of DO-QKD finite-key secure PIE in bpc, assuming that Alice and Bob estimate $\hat{\sigma}_t = 1.1\sigma_{\text{cor}}$, their detector timing jitter $T_J = 2\sigma_{\text{cor}}/3$, their system detection efficiency is 93%, and their background count rate is 1 kcps. The security parameter is $\varepsilon_s = 10^{-5}$, the failure probability of the error correction is $\varepsilon_{EC} = 10^{-10}$, and the reconciliation efficiency is $\beta = 0.9$. The average number of SPDC pairs per symbol-frame is $\mu = \{0.119, 0.231, 0.411, 0.607\}$ for $M \in \{8, 16, 32, 64\}$, respectively. Relevant parameters were chosen to match the asymptotic examples in Ref. [2].

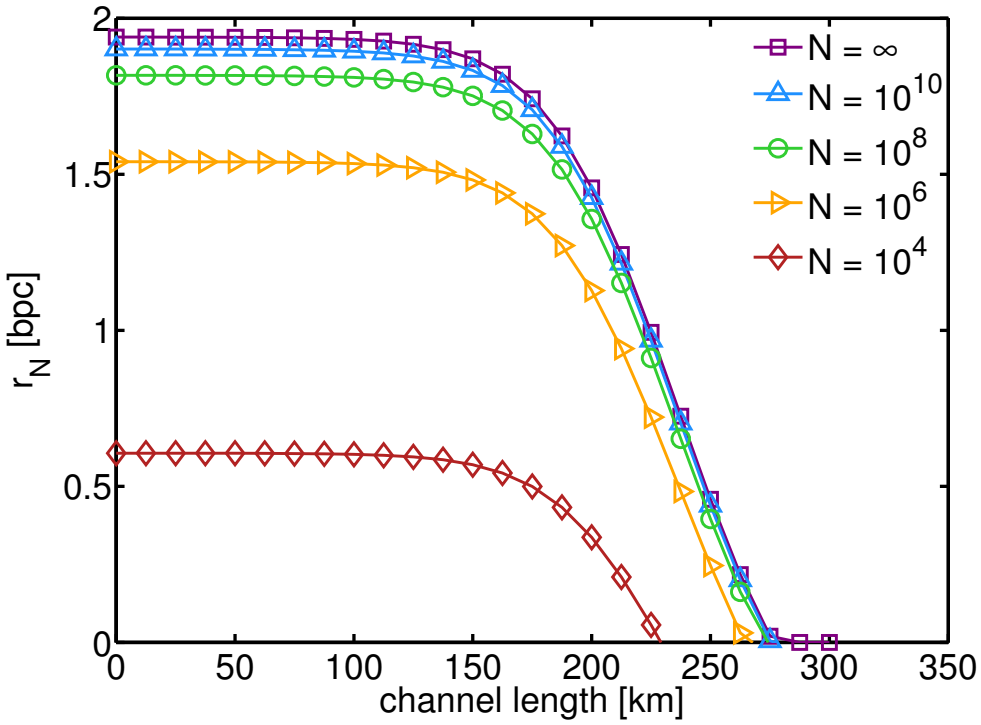

Figure 3-4: Finite-key secure PIE in bpc versus channel length for different N. Here, $M = 8$, the channel loss is 0.2 dB/km, and all other parameters take the same values as in Fig. 3-3 and Ref. [2]. From top to bottom: $N = \infty$, $N = 10^{10}$, $N = 10^8$, $N = 10^6$, $N = 10^4$.

selection probability p and compares the secure PIE using asymmetric basis selection to the secure PIE using symmetric basis selection as functions of N for $M = 8$ [72]. p has an effect on the secure PIE through the factor n/N in Eq. (3.14). Choosing $p > 1/2$ clearly boosts the secure PIE, which approaches its asymptotic value as $p \to 1$. In the symmetric case, where $p = 1/2$, Alice and Bob have on average only $N/2$ coincidences that were measured in the same basis, and only the $n = N/4$ coincidences detected using the TB contributed to the key. When $p = 1/2$, the maximum possible secure PIE, even for large N, reaches only 25% of the maximum, asymptotic value. For all N that yield a positive secure PIE, it is optimal to choose $p > 1/2$. However, the value of p does not change the minimum N required to obtain a positive secure PIE.

3.3.5 Discussion

We have shown security against arbitrary collective attacks for DO-QKD in the finite-key regime, and we can continue to use this security analysis for our experiments. For the example parameters [2], Alice and Bob can reach $> 90\%$ of the asymptotic secure PIE for an experimentally feasible number of detected coincidences, $N \approx 10^7$, and a positive secure PIE is obtained after detecting as few as $N \approx 10^4$ coincidences.

These threshold values of N are on par with the finite-key performance of discrete-variable QKD [23, 156, 157, 159, 165]. In contrast, CV QKD protocols require more measurements; for realistic parameter values, secure information is not obtained until $N \approx 10^8$ [158, 170]. At zero loss, assuming collective attacks, some CV protocols can achieve a positive secure PIE starting at $N \approx 10^6$, but the threshold N increases rapidly as the loss increases; at 25% loss, $N > 10^8$ is required [154].

Although DO-QKD adapts the covariance matrix-based security analysis of Gaussian CV QKD protocols, treating time and frequency as discretized continuous variables to obtain a secure PIE > 1 bpc, its performance under finite-key constraints more closely resembles that of discrete-variable QKD. This is because DO-QKD relies on postselecting detected photon coincidences and thus does not suffer from loss-induced noise like CV QKD. Most importantly, the secure PIE of DO-QKD is not

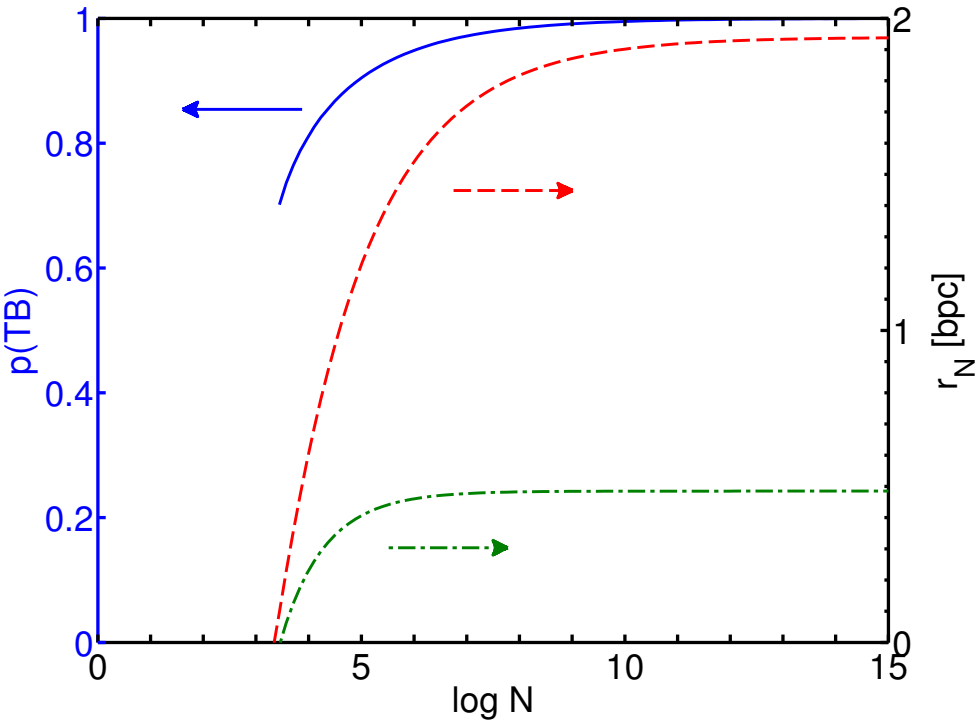

Figure 3-5: Numerically optimized value of p = probability of choosing the TB assuming asymmetric basis selection (solid blue curve), for $M = 8$, alongside a comparison of the secure PIE in bpc assuming asymmetric basis selection using this p (dashed red curve) and symmetric basis selection (dash-dotted green curve). For all N, the secure-key capacity is maximized by choosing $p > 1/2$. Using symmetric basis selection, the secure PIE is limited to 25% of the asymptotic value.

degraded by loss, even in the finite-key regime. This finite-key analysis further highlights the advantages of combining CV and single-photon QKD.

Chapter 4

Prepare-and-measure dispersive optics quantum key distribution

In this chapter, we describe the P&M implementation of DO-QKD, the MIT-LL deployed-fiber testbed, and demonstrations of P&M DO-QKD both in the lab and over the deployed fiber. Our demonstrations achieved record secret-key rates for each channel loss tested [76].

4.1 Motivation

High-dimensional encoding is possible in a variety of degrees of freedom, and large-alphabet QKD has been demonstrated in the laboratory using position-momentum [62], spatial modes in multicore fibers [63, 64], time-energy [4, 52, 65, 67, 71, 75], and OAM modes [77–79]. Of these, time-energy encoding is appealing for its compatibility with existing telecommunications infrastructure — which lowers the barriers to widespread adoption of QKD. The time-energy correlations are robust over transmission in both fiber and free-space channels and are preserved in the presence of WDM systems.

In high-dimensional temporal encoding, the position of a photon within a temporal frame comprising M time slots can convey as much as $\log_2 M$ bits of information, as depicted in Fig. 4-1(a). Classically, this encoding is known as pulse position mod-

ulation (PPM), and combined with single-photon detection, it achieves near-optimal performance in terms of bits per detected photon [171]. Assuming a constant slot duration, PPM exhibits a trade-off between the alphabet size M and the transmitted symbol rate: an increase in the former directly corresponds to a decrease in the latter. The alphabet size determines how much information is encoded in each photon, and the transmitted symbol rate directly impacts how many photons are received per second. We take advantage of this trade-off to maximize the secret-key rate in the presence of receiver saturation.

Fig. 4-1(b) is a representative plot of secret-key rate versus channel length for binary encoding with realizable parameters. Three regimes of distance/loss are indicated. In normal operation (Region II), the secret-key rate decreases exponentially with distance until the received photon flux is comparable to the background counts of the detector(s). At distances/losses beyond this cutoff point (Region III), the correlations between sender and receiver are masked by the background and the secret-key rate drops abruptly. However, at short distances, i.e., low losses (Region I), the secret-key rate is limited when some component of the receiver hardware — such as the detectors or the readout electronics — is saturated by the incoming photon flux, as illustrated in Fig. 4-1(b). In this regime, which extends to approximately 100 km for these parameters, the best strategy to maximize the secret-key rate is to reduce the transmitted photon rate by increasing the alphabet size until the receiver is just below saturation. Although much research has focused on extending the range of QKD links well beyond 100 km [8, 134, 172, 173], shorter links should not be ignored — even at distances ≈ 40 km, secret-key rates lag behind classical data communication rates by orders of magnitude [3, 59]. Futhermore, deployed QKD networks will include a variety of link lengths with potentially different optimal technologies; thus, we focus here on using high-dimensional encoding to maximize secret-key rates over metropolitan-area distances of tens of kilometers.

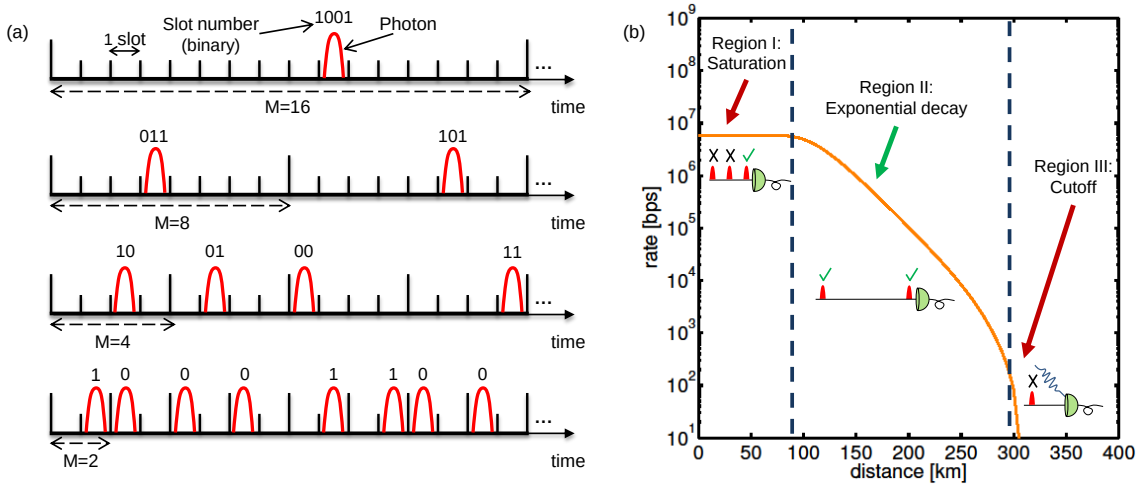

Figure 4-1: (a) In high-dimensional temporal encoding (pulse position modulation), information is encoded in the position of an optical pulse within M slots, depicted here for alphabet size $M \in \{2, 4, 8, 16\}$. For a fixed slot duration, the alphabet size and the transmitted pulse rate are inversely proportional. (b) Representative plot of secret-key rate versus channel length for a traditional two-dimensional QKD protocol, assuming a 5 Gbps modulation rate, a 0.2 dB/km channel loss, a 1 kcps background count rate, a 93% detector efficiency, and a 100 ns detector reset time after each detection event. Three regions are denoted: I. At short distances, 0-100 km (or correspondingly, low losses, 0-20 dB), the secret-key rate is limited by detector saturation. II. For higher losses (normal operation), the secret-key rate decays exponentially with distance. III. At even higher losses ($>$ 300 km), a cutoff is reached when Bob's received photon rate becomes comparable to his detectors' background count rate. The error rate grows and the secret-key rate drops abruptly.

4.2 Prepare-and-measure implementation

In the P&M implementation of DO-QKD, Alice holds a broadband light source, such as a superluminescent diode (SLD), and filters it to the order of 0.1 nm of spectral bandwidth. Alice uses PPM, a programmable pulse pattern generator (PPG), and an electro-optic modulator (EOM) to encode a data pattern that will become the raw key. To transmit in the TB, Alice sends the PPM signal to Bob, and in the FB, she applies GVD to the signal before sending it to Bob. Alice should use a random basis for each transmitted symbol, or more specifically, the basis choice for each symbol must appear random to Eve, and Alice must also record which basis was used for each symbol. In EB QKD, the basis choice is often indicated by which detector fired, making it easy to glean which-basis information from Alice's or Bob's recorded measurements. In P&M DO-QKD, Alice could select a basis for each symbol using active optical switches that deterministically route a pulse through GVD in one arm or, in the other arm, a variable optical attenuator (VOA) to match the insertion loss of the GVD element. After the two arms are recombined, Alice applies extra GVD to precompensate for the dispersion incurred over the fiber channel, and she uses another VOA to keep the average number of photons below one per pulse.

Bob makes the same TB or FB measurements as in the EB DO-QKD protocol; his random basis choices can be implemented using a passive splitter. The essential components of the P&M DO-QKD transmitter and receiver are shown in Fig. 4-2.

Alice's second VOA is operated at multiple preset levels of attenuation, corresponding to different intensities for the signal state, which is used for generating secure key, and one or more weaker decoy states, which are used for channel monitoring to guard against PNS attacks [130, 131, 174–176]. As with the basis choice, Alice's intensity for each transmitted symbol should appear random to Eve, and Alice must record which intensity was used for each symbol.

To aid the sifting, Alice can also transmit a synchronization signal to Bob. An auxiliary ouput of the PPG is used to drive another EOM that carves the cw output of a laser diode into periodic sync pulses. At Bob's receiver, the pulses are detected

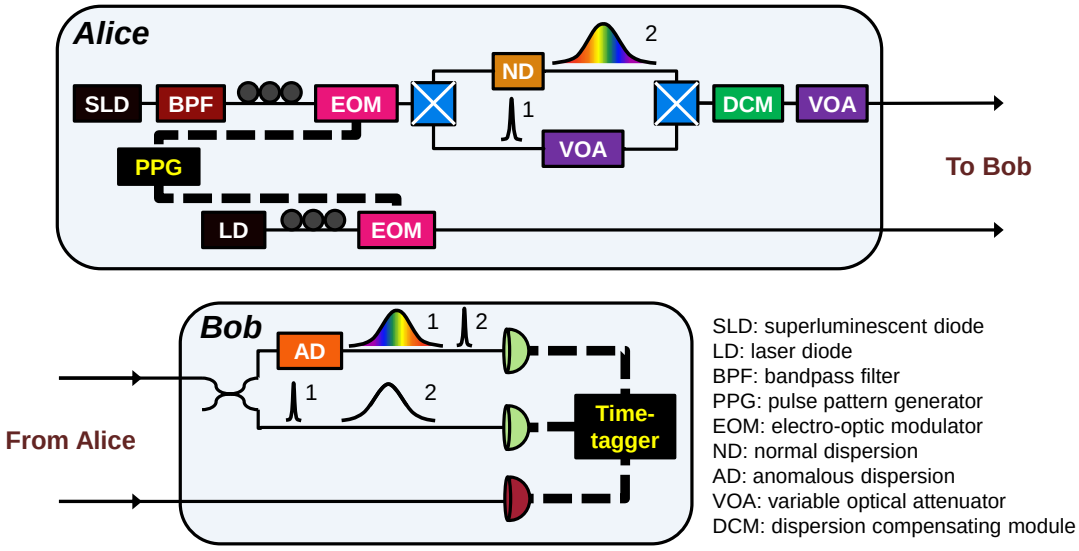

Figure 4-2: Schematic of the P&M DO-QKD protocol. Alice's light source is a filtered SLD; she uses an EOM driven by a programmable PPG to encode the raw key. Active optical switches allow Alice to deterministically route the signal to one of two arms that implement the basis choice: in the upper arm (FB), GVD is applied, and in the lower arm (TB), the signal is attenuated to match the insertion loss of the GVD element. Alice precompensates for the dispersion in the channel and attenuates the signal to the appropriate intensity for either signal or decoy pulses before transmitting it to Bob. Alice uses a second modulator and an auxiliary output of the PPG to produce periodic synchronization pulses that are also transmitted to Bob. Bob detects the synchronization pulses classically, and he detects the quantum signals using the same measurement setup as in the EB DO-QKD protocol. Thin, solid lines indicate optical connections, and thick, dashed lines indicate electrical connections.

classically using an avalanche photodiode (APD). The sync signal is used to determine the symbol and slot edges during sifting, i.e., when Bob demodulates the PPM signal.

The experiments described here are only a proof of principle because Alice's setup differed from an ideal P&M QKD transmitter in several important aspects:

- The raw key data encoded by Alice must come from a trusted source of random numbers; however, we deterministically encoded a repeating pattern of symbols to simplify the PPM demodulation.

- Alice's basis choice for each frame must also come from a trusted source of random numbers (she is allowed to use asymmetric basis switching), and she must know which basis was used for each transmitted frame (for example, using active optical switches, as depicted in Fig. 4-2); however, we used manual basis switching: Alice and Bob used the same basis for an entire dataset, and we combined datasets to perform the key generation and the security checks, because of constraints in the available hardware and the added complexity of the driving and time-tagging electronics.

- Alice's choice of photon intensity, i.e., her choice whether to transmit a signal or a decoy state, must also come from a trusted source of random numbers, and she must know which intensity was used for each transmitted frame (for example, using a programmable VOA or by inserting another EOM to control the intensity of the cw light that reaches the PPM-encoding EOM); however, we used manual decoy states: Alice used the same intensity for an entire dataset, and we combined datasets to perform the key generation and the security checks, again because of constraints in the available hardware and the added complexity of the driving and time-tagging electronics.

We emphasize that these experimental simplifications relate to problems of classical engineering and do not detract from the quantum aspects of this work. A dedicated field-programmable gate array (FPGA) could have simplified the sifting and clock recovery; however, we chose to work with available COTS time-taggers (Picoquant

HydraHarp 400) and perform as many postprocessing tasks as possible using software. Similarly, a custom FPGA could have aided with implementing and tracking Alice's random data/basis/intensity choices; however, we chose to work with a COTS PPG, which provided a mechanism for Alice to drive but not easily track her random outputs. Additionally, at the time of the experiments, only one optical input to a detector array was available. There are precedents for deterministic raw key encoding, manual basis switching and manual decoy states in early proof-of-principle demonstrations of other QKD protocols [177, 178].

4.2.1 Security proof modifications

In EB DO-QKD, Alice and Bob estimate σ_ω, the two-photon spectral correlation [71], by measuring the timing correlations between their photons measured in the FB. For P&M DO-QKD, we use an alternate formulation of ξ_ω. It is more experimentally relevant to measure how well the GVD applied to a PPM pulse is cancelled in the FB, and thus, we want to minimize $\sigma_\omega'^2 \equiv \sigma_\omega^2 - \sigma_{\omega_0}^2$, where again σ_ω represents the two-photon spectral correlation width including Eve's effects, and σ_{ω_0} is the noiseless spectral correlation. To clarify, the measured σ'_ω is related to the *increase* in the two-photon spectral correlation width, and not to the width itself. Keeping the definition of ξ_ω from Eq. (3.8), we can rewrite ξ_ω in terms of the experimentally measured σ'_ω as

$$\xi_\omega = \frac{\sigma_\omega'^2}{\sigma_{\omega_0}^2}. \tag{4.1}$$

We can use the same finite-key analysis presented in Section 3.3.3 to obtain worst-case estimates for σ'_ω and ξ_ω.

Finally, the secure PIE is revised. Since only Bob detects photons, no photon coincidences are recorded; thus, the units of the secure PIE become bits per detected photon (bit/photon), or simply bits. Decoy-state analysis must be added to the calculation of the secure PIE [175]. In the asymptotic regime, the secure PIE including

decoy-state analysis is

$$r_{\infty,\text{decoy}} = \beta I(A;B) - (1 - F_\mu^{\text{LB}}) \log_2 M - F_\mu^{\text{LB}} \chi^{\text{UB}}(A;E), \tag{4.2}$$

where F_μ^{LB} is a lower bound on the fraction of Bob's detection events that came from a single-photon transmission by Alice and $\chi^{\text{UB}}(A;E)$ is an upper bound on the Holevo information. Decoy-state measurements contribute to the estimation of F_μ^{LB} and $\chi^{\text{UB}}(A;E)$. In the finite-key regime, we must also consider the effects of a finite sample size on the estimation of the parameters related to decoy states [176], in addition to the penalty terms from Eq. (3.14) and the impact on the Holevo information.

4.3 Deployed-fiber testbed

For field tests of this and other quantum networking applications, we have established a 42-km deployed-fiber testbed in collaboration with LL. The testbed comprises two strands of dark (i.e., carrying no other light) fiber running in parallel between the main campus of MIT in Cambridge, MA, and LL in Lexington, MA, as approximately illustrated in Fig. 4-3. Compared to the same length of fiber on a spool in the lab, installed fibers have higher losses due to large numbers of splices and bends.

The loss can be measured using a laser and an optical power meter, but greater information is given by an optical time domain reflectometer (OTDR). OTDRs transmit pulses and measure and time the backscattered power to determine the location and loss of splices in an optical fiber. An OTDR measurement requires access to only one end of the fiber, making it a convenient tool for characterizing deployed fibers. Fig. 4-4 shows a representative OTDR trace of one of the deployed fibers, as measured from the LL end.

The loss over the deployed fiber fluctuates from day to day. For a quasi-long-term measurement of the round-trip loss, the output of a cw laser was split at LL; half of the power was monitored by a local power meter while the other half traversed down one of the dark fibers to MIT, through a short jumper, and back to LL over the other

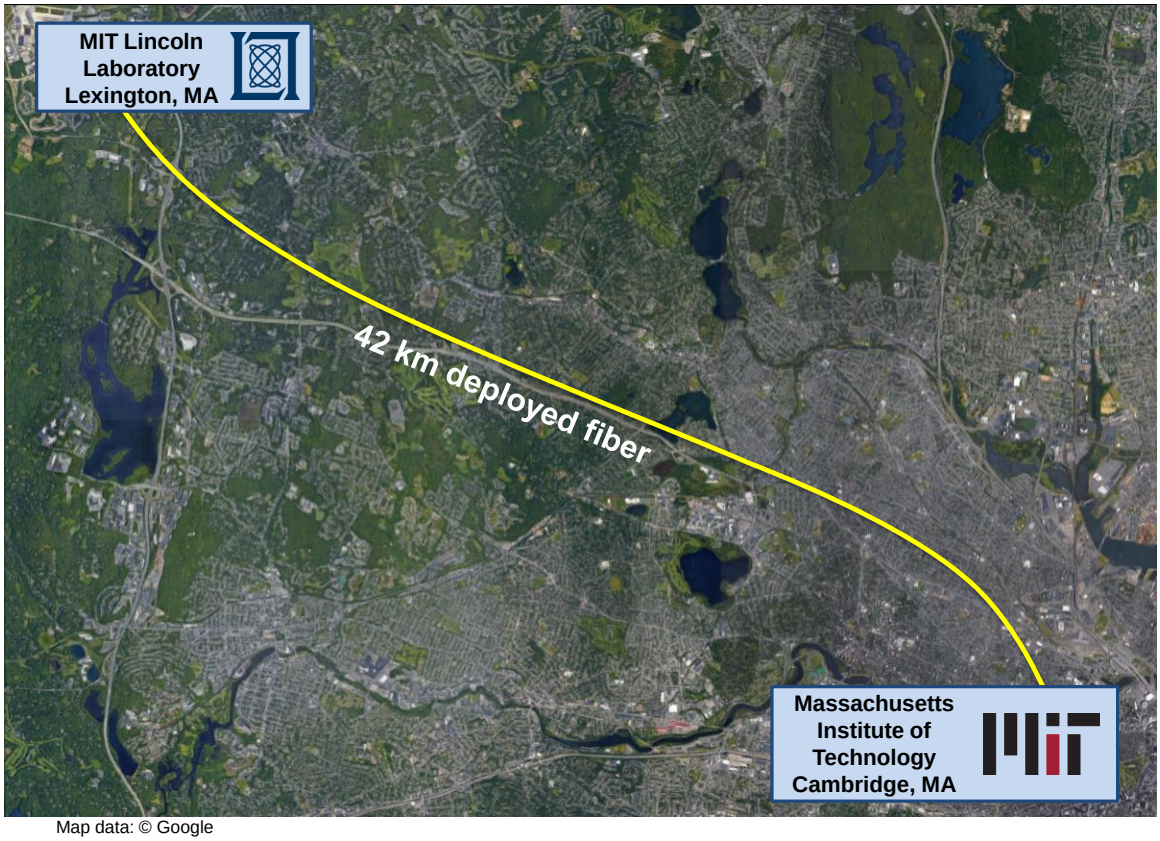

Figure 4-3: Illustration of the MIT-LL deployed-fiber testbed. Locations of MIT and LL are accurate, but the fiber path is an artistic rendering because information about the exact path is not currently accessible.

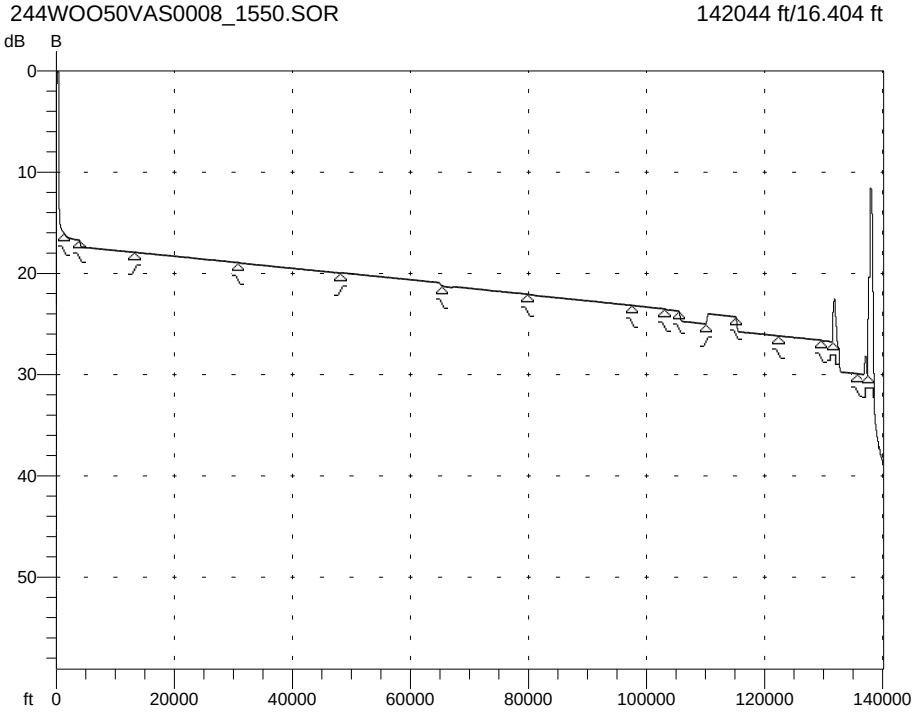

Figure 4-4: Representative OTDR trace from LL to campus. The x-axis shows distance in feet; the y-axis shows relative backscattered power in dB. The slope of the trace indicates the loss of the fiber without splices; discontinuities and/or spikes indicate large losses and/or backreflections that are characteristic of splices. Around 110,000 feet, there appears to be a gain in the fiber; this is most likely due to a patch of non-standard (probably dispersion-shifted) fiber that is part of the link.

dark fiber, where it was measured with a power meter. The difference between the readings from the two power meters, recorded over four days in August 2014, is plotted in Fig. 4-5. Large swings of about 0.1 dB appear on weekdays but not on weekends. Some of the observed fluctuations could be related to polarization drifts over the fiber and polarization-dependent loss at the power meter. The cause of the long-term average drift toward lower loss is currently unknown. Besides small-scale fluctuations like those shown in Fig. 4-5, the one-way loss varies on the order of dB from day to day, over months and years. One-way loss measurements are conducted by measuring the power of a cw laser at one end of the fiber (usually at MIT), sending the light over the deployed fiber, and measuring the received power at the other end (usually at LL). The power meters on either end of the fiber may not be identically calibrated, but the observed variation in loss is too large to be solely attributed to calibration differences or the non-repeatability of connecting two FC/PC fiber connectors. At the time of the demonstration reported in this chapter, the measured loss was 12.7 dB — equivalent to 63.5 km of standard single-mode fiber on a spool (assuming standard loss of 0.2 dB/km). In December 2016, one of the fibers broke; after it was repaired, the loss increased to ~ 16 dB.

For DO-QKD, we are particularly interested in the dispersion of the deployed fiber. The dispersion incurred over the fiber channel must be properly compensated (or at least quantified), or the security analysis of the protocol would be affected. To characterize the one-way dispersion, the output of a pulsed laser was transmitted over the fiber from MIT to LL. At LL, the received power was first amplified by an erbium-doped fiber amplifier (EDFA) and then split; the pulses in each arm were passed through a bandpass filter with a tunable center wavelength before being detected classically by a photodiode. The center wavelength of one bandpass filter was fixed while the other was swept through the wavelength region of interest (approx. 1559-1563 nm). The relative delay between the detected pulses was recorded using an oscilloscope. This delay is plotted as a function of the center wavelength of the swept filter in Fig. 4-6. The quantity of interest, the GVD induced by the deployed fiber, is the slope of the delay-vs.-wavelength line, and its value is 693 ps/nm.

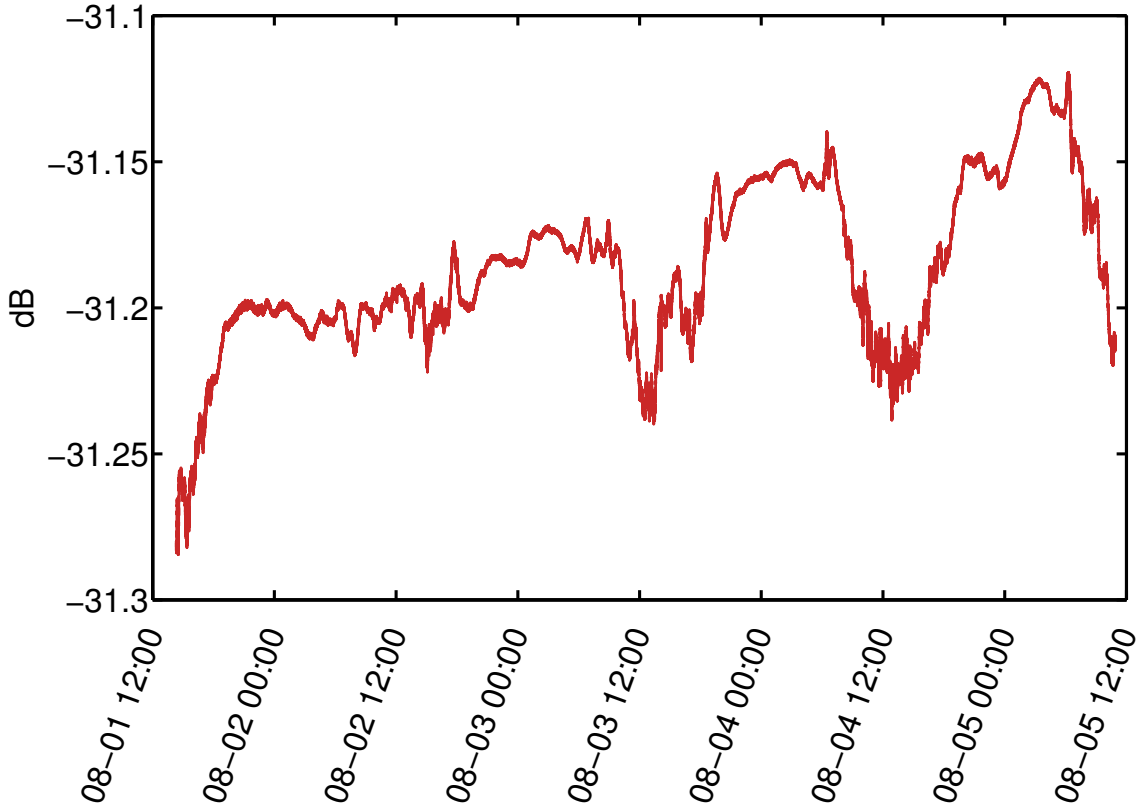

Figure 4-5: Round-trip loss over the deployed fiber, as recorded at LL from Friday, August 1, 2014 to Tuesday, August 5, 2014. On weekdays, there is a large swing of nearly 0.1 dB with a period of about one day. The cause of the average upward (toward lower loss) drift is unknown.

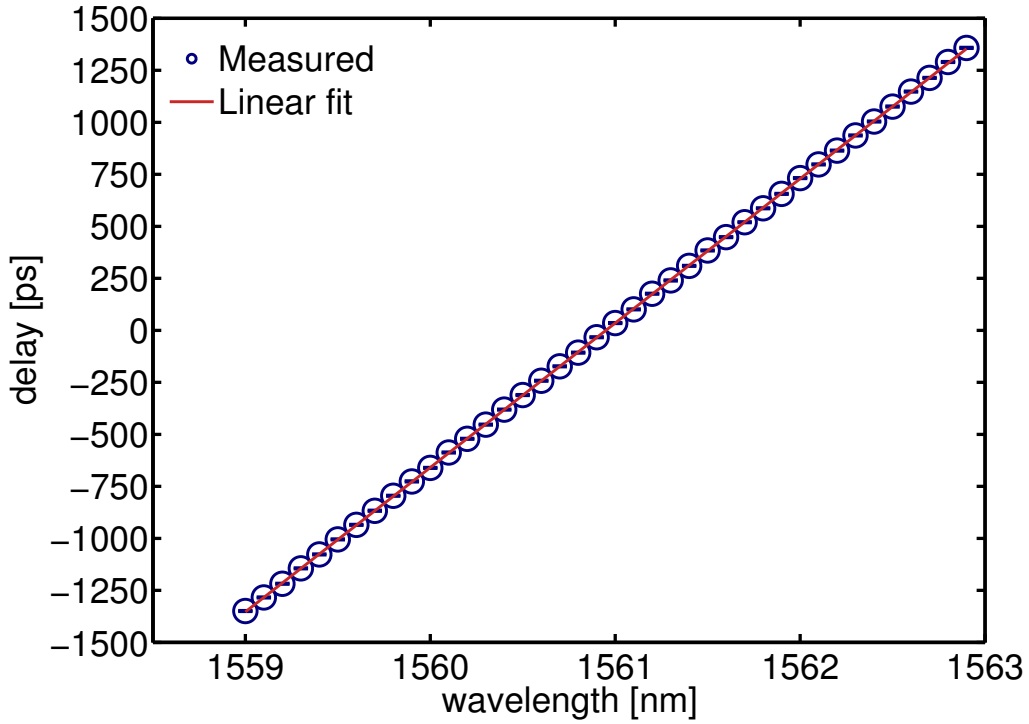

Figure 4-6: One-way dispersion over the deployed fiber, measured by recording the delay experienced by pulses transmitted from MIT to LL. The size of the error bars was determined by the uncertainty in reading the delay from the oscilloscope. The quantity of interest is the slope of the linear fit, 693 ps/nm.

An arguably more precise method to characterize chromatic dispersion in optical fibers is by measuring the phase shift experienced by a sinusoidally modulated cw laser as its wavelength is tuned [179, 180]. However, this method requires simultaneous access to both ends of the fiber, which the deployed fiber does not allow. This method was used to characterize the 41-km fiber spool that was used to test the P&M DO-QKD system; the measured dispersion was 685 ps/nm.

4.4 Results

We implemented a proof-of-principle demonstration of P&M DO-QKD. All components of Alice's and Bob's setups, apart from Bob's single-photon detectors, were commercially available. Bob's single-photon detectors were niobium nitride (NbN) superconducting nanowire single-photon detectors (SNSPDs) capable of counting at hundreds of Mcps rates, with timing resolution of tens of picoseconds and few kcps dark count rates [181]. Bob had access to four NbN nanowires that are interleaved in a circular array and illuminated by a single optical fiber. Because the entire quad of nanowires has only one optical input, the quad is effectively one detector. The effective effiency of this single detector was 68%. With only one detector, Bob could not easily measure in both the TB and the FB during the same data acquisition interval, so Bob retained the same basis for the duration of each interval (on the order of 1-10s of minutes, depending on the received photon flux). However, although the quad has only a single optical input, each of the nanowires in the quad has its own RF output, each of which is timetagged using a Picoquant Hydraharp with 1 ps timing resolution. The four nanowires do not have the same timing jitter, so the sifting and security checks for each nanowire were processed separately in software.

Just as Bob used a single basis for an entire data acquisition interval, Alice also used a single basis, as well as a single intensity, for an entire interval. Alice transmitted signal pulses with average intensity $\mu = 0.5$ photons per pulse and decoy pulses with average intensity $\nu = \mu/10 = 0.05$ photons per pulse. The pulses were ~ 50 ps FWHM, as verified using a classical photodiode. The light source was an SLD filtered

to 0.2 nm (25 GHz). The pulses were produced using a lithium niobate EOM driven by a programmable PPG (Anritsu MP1763B). The 50-ps pulses were centered in slots of duration 240 ps. M slots comprised a symbol, with $M \in \{4, 8, 16, 32\}$. Between each M-slot symbol, an additional two guard slots were included to act as buffers.

Different datasets corresponding to Alice's and Bob's different choices of intensity and basis were combined using software. Numerical optimization (implementated in MATLAB) determined the effective fraction of time for each person to use each basis and intensity to maximize the secret-key rate. The finite-key security parameter used in the optimization was $\varepsilon_s = 10^{-10}$, which is the standard value chosen in several other experiments [8, 59, 112, 113].

To implement the FB measurements, custom GVD elements with $\pm 10,000$ ps/nm of dispersion were manufactured by Proximion AB. The operating principle is based on chirped fiber Bragg gratings (FBGs) that introduce wavelength-dependent time delays. Compared to the length of standard single-mode fiber required to effect the same magnitude of dispersion (588 km @ 17 ps/nm/km and 0.2 dB/km), the insertion loss of these FBG-based elements is significantly lower (< 4 dB).

The P&M DO-QKD system was tested with three different channel configurations:

1. Alice and Bob were both located at LL, connected by a short patch cable with negligible loss (the "back-to-back" configuration).

2. Alice and Bob were both located at LL, connected by a 41-km spool of standard single-mode fiber with 7.6 dB loss. Alice's transmitter included a spool of dispersion-compensating fiber (DCF) to precompensate for the GVD of the 41-km spool.

3. Alice was located at MIT and Bob was located at LL. They were connected by the 42-km deployed fiber, which, on the day of the demonstration, was measured to have 12.7 dB loss. Alice's transmitter again included the same spool of DCF to precompensate for the GVD of the deployed fiber. The quantum signals were transmitted over the strand of dark fiber with lower loss, and the periodic sync pulses were transmitted over the other strand to eliminate crosstalk between

	Back-to-Back	41-km spool	42-km deployed fiber
Loss (dB)	0.1	7.6	12.7
Optimal M	16	8	4
Max. secret-key rate (bps)	23×10^6	5.4×10^6	1.2×10^6
Secure PIE (bit/photon):			
Nanowire 1	1.46	0.82	0.41
Nanowire 2	1.33	0.79	0.35
Nanowire 3	1.42	0.96	0.60
Nanowire 4	1.37	0.94	0.61

Table 4.1: Summary of the maximum secret-key rates obtained in the three test cases.

the sync and quantum signals.

Table 4.1 summarizes the three test cases. Our results exemplify the rate trade-off inherent to P&M high-dimensional time-energy QKD (and to PPM): for a fixed slot duration, a larger alphabet size M increases the potential secure PIE but decreases Alice's transmitted photon rate. The optimal M to maximize the secret-key rate is a function of Bob's receivable photon rate. Fig. 4-7 displays the secret-key rates obtained for each alphabet size M in the three test cases. The optimal M decreases as loss increases.

We note that in the deployed-fiber case, our measurements alone do not confirm whether $M > 2$ gives a higher secret-key rate than $M = 2$. We did not test the case when $M = 2$ because DO-QKD is not optimal when $M = 2$. The secure PIE presented in Eq. 4.2 holds only against the class of collective attacks, whereas traditional, two-dimensional protocols such BB84 [31] have proven security against the most general, coherent attacks [59]. Furthermore, Eq. 4.2 tends to yield a lower secure PIE than that afforded by BB84. Ref. [59], the highest-rate BB84 demonstration for which secure PIE data is available, obtained 0.26 bit/photon with 10 dB channel loss. At the same loss, a numerical simulation shows that P&M DO-QKD with $M = 2$ achieves a secure PIE of 0.16 bit/photon. The numerical simulation uses the measured parameters (e.g., Alice and Bob's timing correlations, detector timing jitter) of the deployed-fiber test case. Over the deployed fiber with 12.7 dB loss, DO-QKD with $M = 2$ should achieve a secret-key rate of 605 kbps, indicating that increasing M provides a boost in the

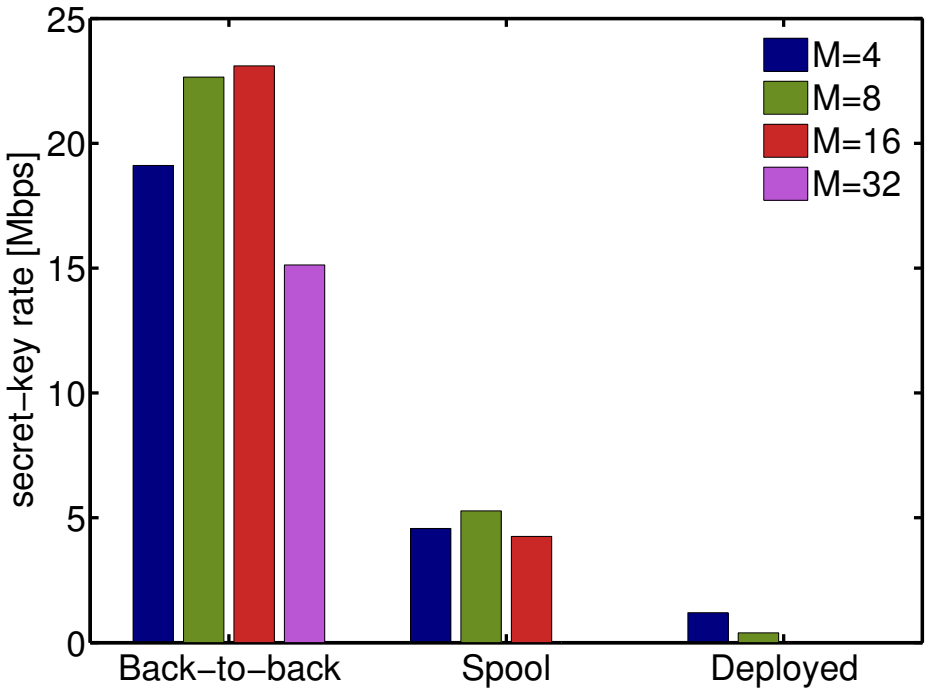

Figure 4-7: Experimental secret-key rates for all measured alphabet sizes of each test case. Loss increases from left to right. The optimal M decreases as loss increases. For experimental convenience, we did not increase the alphabet size once it became apparent that doing so would not increase the secret-key rate.

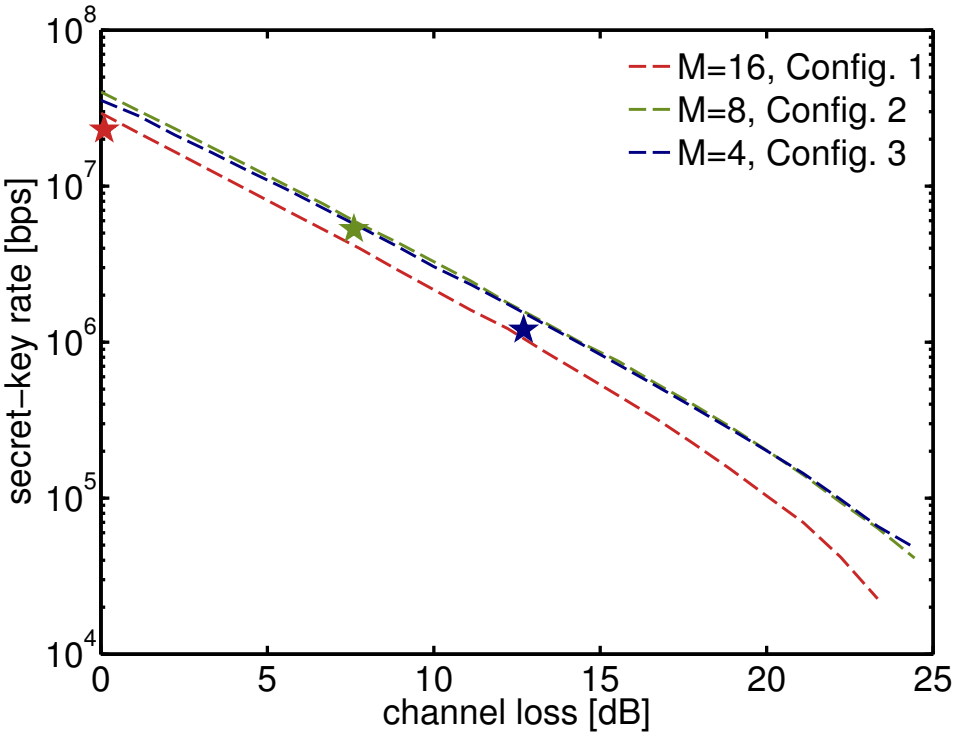

Figure 4-8: Experimental (stars) and theoretical (dashed curves) secret-key rates versus channel loss. Colors correspond to optimal alphabet size M for each of the three test configurations. Each theoretical curve uses a different set of experimental parameters (e.g., detector timing jitter) that corresponds to each of the test configurations: Config 1 = Back-to-back; config. 2 = 41-km spool; config. 3 = 42-km deployed fiber.

secret-key rate.

Results from the same numerical simulation, using the alphabet sizes and measured parameters corresponding to the maximum secret-key rate from each test configuration, are plotted in Fig. 4-8, along with the experimental secret-key rates. The reported values and theoretical curves include decoy state and finite-key analysis with sample size $N = 10^9$ counts and security parameter $\varepsilon_s = 10^{-10}$ [72, 176]. The colors in Fig. 4-8 correspond to alphabet size and thus to test configuration, since each configuration had a different optimal alphabet size. The theoretical curves should not be directly compared to each other because they are based on different experimentally measured values. The theoretical curves are included to show that the numerical simulation behaves qualitatively as expected as a function of channel loss.

4.5 Discussion

The optimal M to maximize the secret-key rate depends most strongly on Bob's received photon rate, which is in turn a function of channel loss. If Bob had an infinitely fast receiver, the highest secret-key rate would be obtained for the fastest transmitter rate, which occurs for $M = 2$. However, Bob's receiver hardware is usually rate-limited. The limit may be due to the single-photon detectors themselves; for instance, SNSPDs exhibit reset times ranging from a few nanoseconds [181–184] to several tens of nanoseconds [184–186], depending on the choice of superconductor. The detector readout electronics can also limit the receiver count rate, as is the case for the commercial time-tagger in our system, which has a dead time of 80 ns per channel, and also for the high-rate BB84 demonstration of Ref. [3].

When Bob's receivable photon rate is limited, increasing $M > 2$ allows Alice and Bob to effectively produce secret keys even during the dead time. Thus, at short distances and correspondingly low losses, we can expect a bottleneck due to the maximum count rate of Bob's receiver.

Our results in Table 4.1 confirm that increased loss between Alice and Bob is correlated with a decrease in the alphabet size that produced the highest secure key rate. Considering the representative plot in Fig. 4-1(b), we expect that at short separations, say from 0-75 km, and correspondingly low losses, 0-15 dB, Bob's detectors are likely to become saturated, meaning that P&M DO-QKD could be particularly advantageous for high-rate QKD on shorter links, on the scale of metropolitan-area networks. Slower receivers would derive greater benefits from the high-dimensional protocol, as saturation would occur at lower incoming photon rates. Fig. 4-9 compares our results to some notable previously published QKD experiments, and we see that P&M DO-QKD currently outperforms the other systems in this low-loss regime.

Additionally, the 1.2 Mbps secure key rate over the deployed fiber is the highest rate reported in a QKD field test to date. Table 4.2 compares this result to other tests over installed fibers with similar losses [112, 187]. However, we note that Refs. [112, 187] feature real-time postprocessing, while our system performs postprocessing in

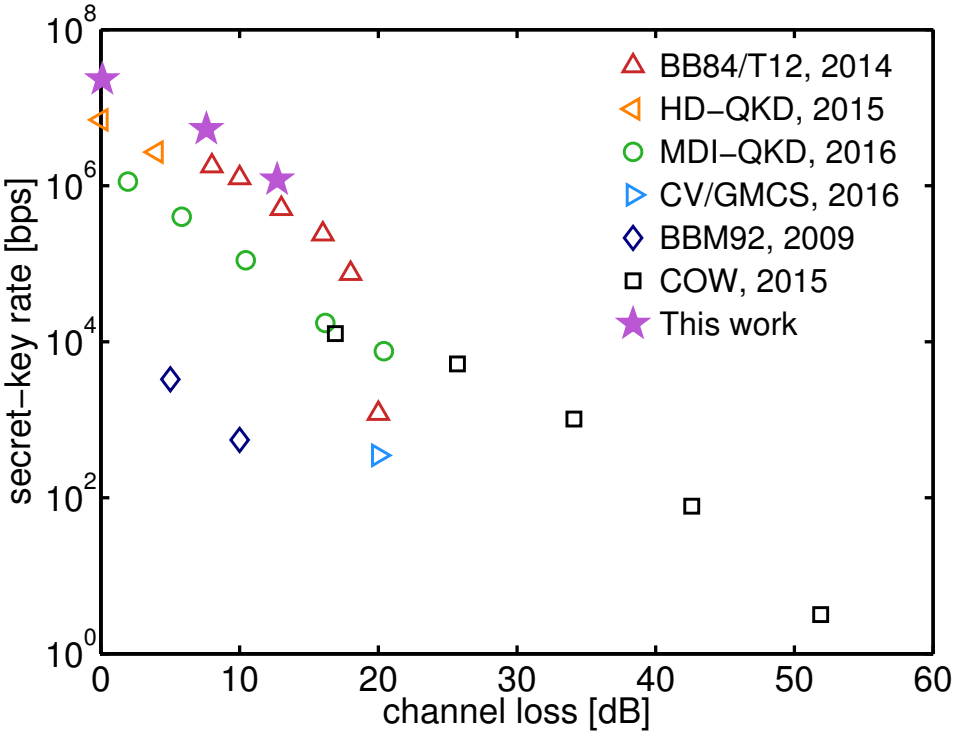

Figure 4-9: Comparison of our P&M DO-QKD results to previously published QKD system records, chosen to represent either secure throughput or distance records for a variety of protocols. BB84/T12: secure throughput record for two-dimensional QKD [3]. HD-QKD: secure throughput record for high-dimensional entanglement-based QKD [4]. MDI-QKD: secure throughput record for measurement-device-independent QKD [5]. CV/GMCS: distance record for continuous-variable QKD [6]. BBM92: secure throughput record for two-dimensional entanglement-based QKD [7]. COW: distance record for QKD [8].

	Ref. [187]	Ref. [112]	This work
Distance (km)	45	45	42
Loss (dB)	14.5	14.5	12.7
Secret-key rate (bps)	0.208×10^6	0.301×10^6	1.26×10^6
Secret-key rate normalized to 10 dB loss (bps)	0.586×10^6	0.848×10^6	2.35×10^6

Table 4.2: Comparison of our P&M DO-QKD results to previously published QKD field tests over installed fibers of similar length. Both comparison works used BB84.

software.

The high-dimensional time-energy encoding demonstrated by P&M DO-QKD offers the ability to optimize the secret-key rate by varying the alphabet size M in response to both receiver capabilities and channel loss. This is most advantageous when Bob's receiver is saturated, which can often occur over metropolitan-area distances of tens of kilometers. By presenting and demonstrating a protocol intended to adapt to the constraints of a particular link implementation, this work represents a new approach to high-rate secure quantum communication optimized for use in metropolitan areas.

Chapter 5

Entanglement-based dispersive optics quantum key distribution

In this chapter, we describe the implementation of EB DO-QKD, including the construction of SPDC source(s), an in-laboratory experiment that is the first demonstration of a high-dimensional QKD protocol with security against arbitrary collective attacks, and steps toward demonstrating EB DO-QKD over the deployed-fiber testbed.

5.1 Spontaneous parametric downconversion source(s)

For completely non-scientific reasons, two different SPDC sources were built: the first on campus and the second at LL. The sources are functionally the same; they are based on similar though non-identical type-II quasi-phased-matched periodically poled potassium titanyl phosphate (PPKTP) waveguides fabricated by AdvR, Inc. The waveguides are designed to convert pump light around 780 nm to orthogonally polarized signal and idler photons at approximately 1560 nm, conserving energy. The signal and idler wavelengths can be tuned over a few nanometers by adjusting the pump wavelength, and because the fabrication is not uniform, different waveguides on the same chip exhibit downconversion over slightly different wavelength ranges. However, in contrast to other SPDC sources, such as those based on periodically

poled lithium niobate (PPLN), temperature tuning has negligible effect on the phase-matching of these type-II quasi-phased-matched waveguides in PPKTP. As a result, for a given waveguide, the wavelength at which the signal and idler are degenerate cannot be shifted.

In both source setups, the pump, signal, and idler beams are free-space coupled into and out of the waveguide. The primary differences relate to separating the pump beam from the daughter photons and splitting the orthogonally polarized signal and idler beams.

5.1.1 Campus source setup

A schematic of the campus SPDC source setup is shown in Fig. 5-1. A half-wave plate (HWP) placed before the PPKTP waveguide input rotates the polarization of the pump beam before the pump is coupled into the waveguide. After the waveguide output, a dichroic mirror reflects most (but not all) of the pump beam while transmitting the signal and idler. Subsequent extinction of the pump is done by dielectric mirrors that have $> 99\%$ reflectivity over telecom wavelengths but do not reflect the 780 nm pump. Any higher-order waveguide modes are removed from the SPDC output beam by a 10 nm bandpass filter (BPF) [86]. The orthogonally polarized signal and idler photons are coupled into the same polarization maintaining (PM) single-mode fiber, which also filters out higher-order spatial modes. The fast and slow axes of the PM fiber are aligned with the signal and idler polarizations, respectively. The signal and idler are then separated using a fiber-based polarizing beamsplitter (PBS). The phase-matching bandwidth of this source is 200 GHz.

Fig. 5-2 plots detected single and coincidence count rates as a function of the pump power measured in free-space before the PPKTP waveguide. The detectors used with the campus source were tungsten silicide (WSi) SNSPDs loaned as part of a collaboration with NIST and JPL. The WSi detectors had system detection efficiencies $> 85\%$, full width at half maximum (FWHM) timing jitters $T_J \sim 80 - 120$ ps, background count rates on the order of $1 - 10$ kHz, and maximum count rates on the order of 1 MHz (values varied based on the specific detector channel). As

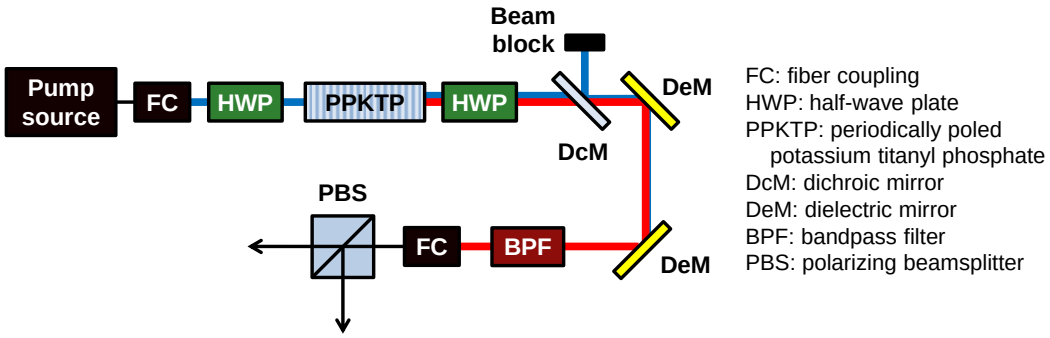

Figure 5-1: Diagram of the campus SPDC source setup. A HWP rotates the pump polarization before the PPTKP waveguide. A second HWP is placed after the waveguide for fine polarization adjustment of the orthogonally polarized signal and idler photons, to maximize the extinction when they are separated by a fiber-based PBS. The pump is extinguished by a combination of dichroic and dielectric mirrors, and the signal and idler photons are coupled into the same PM fiber. Thin, black lines indicate fiber connections; blue lines indicate free-space transmission of the pump beam, and red lines indicate free space transmission of the signal/idler beams.

the photon count rate increases, the observed timing jitter also increases. Fig. 5-2 shows detectable count rates approaching 9 MHz, but because the timing resolution is degraded at high rates, it is better to constrain to the photon rate to ≤ 5 MHz.

5.1.2 Lincoln source setup

The SPDC source at LL was built after the one on campus, and the experience of using the campus source motivated some modifications in the LL setup. A schematic of the LL SPDC source setup is shown in Fig. 5-3. In contrast to the campus setup, the pump side of the LL setup has a quarter-wave plate (QWP) in additional to a HWP. The QWP converts an elliptical polarization to a linear one. It was not needed on campus because the pump source and SPDC setup were directly adjacent to each other, but it is helpful at LL, where one of the pump sources (futher described in Section 5.1.3) is located on a different optical table and connected to the SPDC source by 15 m of non-PM fiber. To separate the pump from the signal and idler beams, the dichroic mirror from the campus setup is replaced by two identical longpass filters (LPFs) that have both greater extinction of the pump and higher transmission of the outputs.

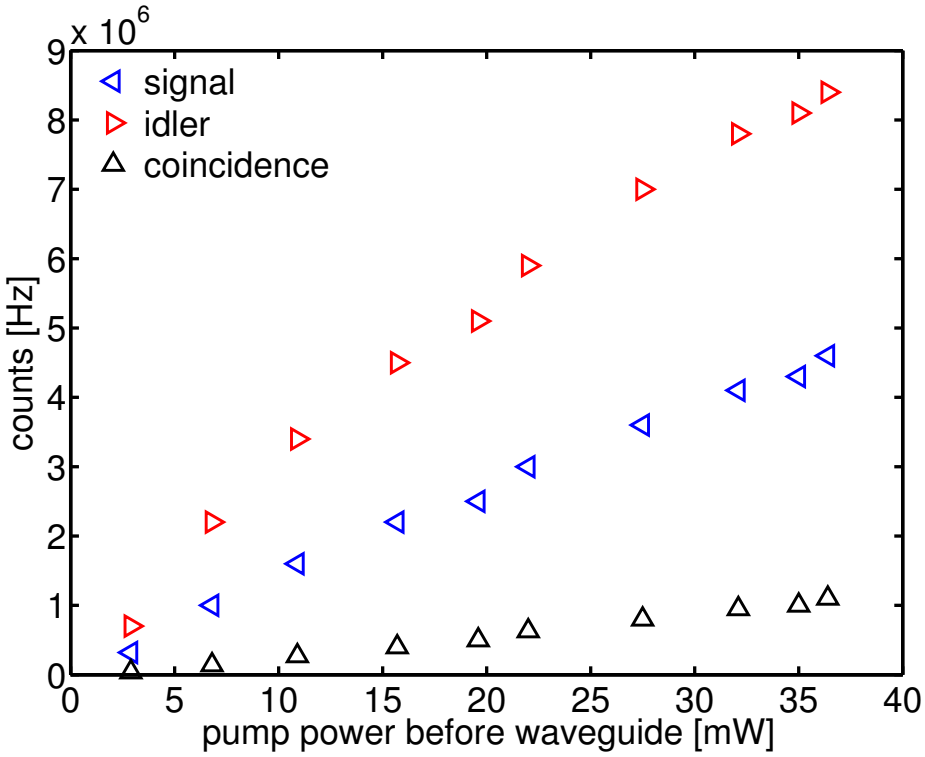

Figure 5-2: Singles and coincidence count rates as functions of pump power for the campus SPDC source, detected using WSi SNSPDs.

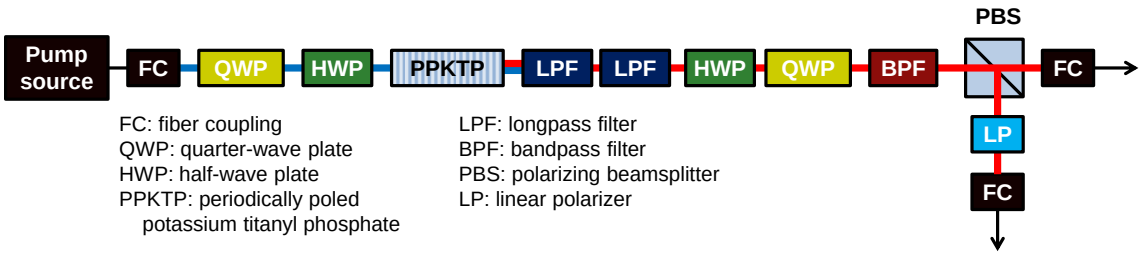

Figure 5-3: Diagram of the LL SPDC source setup. A QWP and a HWP adjust the pump polarization before the PPTKP waveguide. The pump is blocked by two identical LPFs. A second HWP and QWP are placed after the waveguide for fine polarization adjustment of the orthogonally polarized signal and idler photons, to maximize the extinction when they are separated by a free-space PBS before being coupled into separate PM fibers. A linear polarizer on the output of the reflected port of the PBS improves the polarization extinction. Thin, black lines indicate fiber connections; blue lines indicate free-space transmission of the pump beam, and red lines indicate free space transmission of the signal/idler beams.

The LPFs are followed by a HWP and QWP for fine-tuning of the polarization and then the same 10 nm BPF for cleaning up higher-order spatial modes. A free-space PBS separates the signal and idler with greater extinction than the fiber-based PBS from the campus setup, and a linear polarizer provides additional suppression of the unwanted polarization at the reflected output of the PBS. The signal and idler photons are coupled into separate PM fibers. The fiber coupling can be optimized individually for each of the signal and idler beams to maximize the detected coincidence rate. The phase-matching bandwidth of this source is 375 GHz.

Fig. 5-4 plots detected single and coincidence count rates as a function of the pump power measured in free-space before the PPKTP waveguide. The pump was a cw laser, and the detectors were quads of NbN SNSPDs, as described in Section 4.4. However, only two nanowires from each quad were connected to the timetagger (effectively reducing the detection efficiency of each quad by 1/2).

5.1.3 Pulsed pump source(s)

Both SPDC source setups require a fiber-coupled 780 nm pump. For alignment and characterization, we typically use a fiber-coupled tunable cw laser, but some DO-QKD

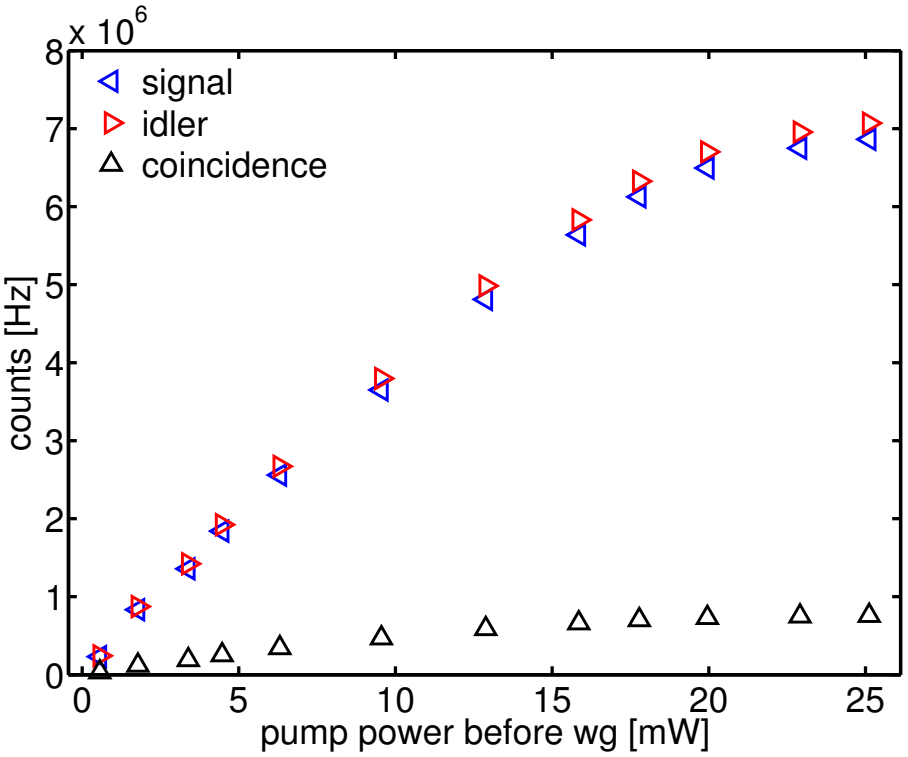

Figure 5-4: Singles and coincidence count rates as functions of pump power for the LL SPDC source, detected using NbN SNSPD quads.

experiments call for pump pulses with FWHM duration $\sim 1-10$ ns. On campus, this was accomplished by using a lithium niobate ($LiNbO_3$) EOM to carve the 780-nm cw light into pulses of the desired duration. However, the average output power was only $\sim$ 3 mW. This was partially due to the low pulse duty cycle ($\sim$ 1% for this experiment), which we could have changed, but the other constraints on the output power came from the EOM's high insertion loss and the susceptibility of $LiNbO_3$ to photofractive damage at wavelengths < 1 μm. Additionally, the EOM's low extinction ratio ($\sim$ 10 dB, measured indirectly by detecting the downconverted photons) meant that the EOM did not sufficiently block the laser when the pump should have been "off."

At LL, we were able to take advantage of existing hardware to improve the pump pulse extinction ratio and increase the average output power. The full setup of the improved pulsed pump source is illustrated in Fig. 5-5. An arbitrary waveform generator (AWG) was used to produce RF Gaussian pulses at a higher repetition rate (31.25 MHz). These RF pulses were amplified and used to drive a telecom-band $LiNbO_3$ EOM that was in all ways superior to the short-wavelength one: thanks to significant investment in research and development motivated by the telecom industry, COTS $LiNbO_3$ EOMs are available at telecom wavelengths with high extinction and low insertion loss. The pulses thusly produced at 1560 nm were first amplified by two stages of EDFAs to an average power > 3 W and then upconverted by second harmonic generation (SHG) in a bulk PPLN crystal to produce Gaussian pulses with high extinction at 780 nm. The measured SHG conversion efficiency was 5 %/W. The average in-fiber power of the SHG pulses exceeded 20 mW; this power was subsequently attenuated as desired to pump the SPDC source. The PPLN setup was previously designed, built, and aligned by Ben Dixon, Ryan Murphy, and Margaret Pavlovich; it happened to be sitting in the lab unused, and thus we were able to quickly incorporate it into the SPDC system with only some minor adjustments.

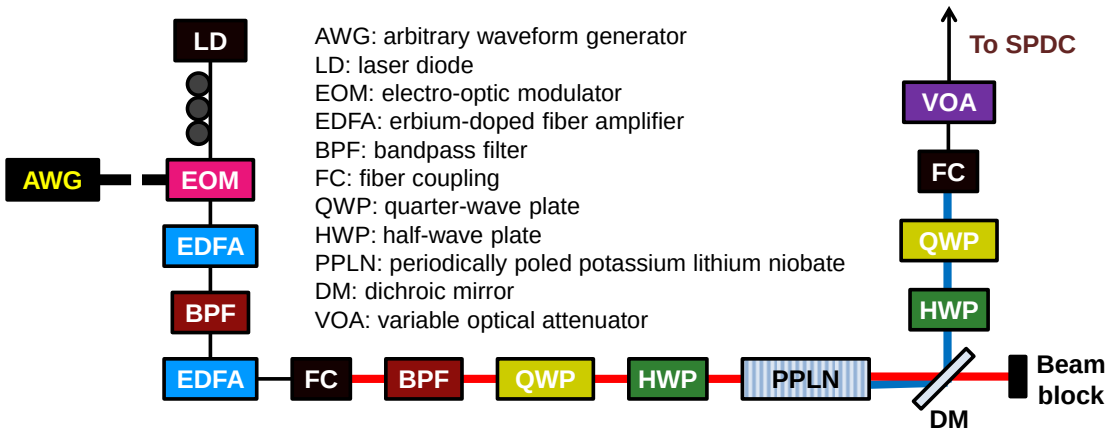

Figure 5-5: Diagram of pulsed SHG source. Gaussian RF pulses produced by an AWG are used to drive a lithium niobate EOM, producing Gaussian optical pulses at 1560 nm. The telecom pulses are amplified by two cascaded EDFAs, with a BPF between the first and second stages to elimate unwanted amplified spontaneous emission. After being launched into free space and passing through another BPF, the average optical power is > 3 W. A QWP and HWP adjust the telecom pump polarization before the bulk PPLN crystal. After the PPLN, the telecom and SHG are separated by a DM, and after polarization adjustment by a HWP and QWP, the SHG is coupled into fiber. A fiber-based VOA controls the SHG power that is sent to the SPDC source. Thick, dashed lines indicate electrical connections; thin, black lines indicate fiber connections; red lines indicate free space transmission at 1560 nm; and blue lines indicate free-space transmission at 780 nm.

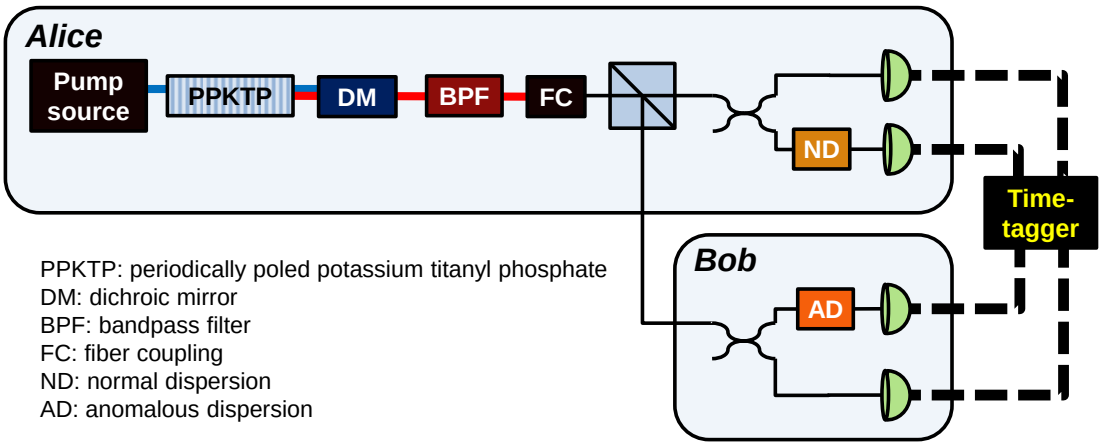

Figure 5-6: Experimental setup for the EB DO-QKD demonstration with Alice and Bob located in the same lab, which allows them to share a single timetagger. The SPDC source is simplified in this illustration. Thin, solid lines indicate optical connections; thick, dashed lines indicate electrical connections; blue lines indicate free-space transmission of the pump beam; and red lines indicate free space transmission of the signal/idler beams.

5.2 Lab demonstration of entanglement-based dispersive-optics quantum key distribution

The in-lab demonstration of EB DO-QKD occurred on campus using the campus SPDC source and the NIST/JPL WSi SNSPDs. The photon detection efficiency from source to detector was 3.3% and 0.77% for Alice and Bob, respectively, including all coupling losses. Fig. 5-6 shows a schematic of the EB DO-QKD setup for this demonstration. Whenever Alice and Bob are located in the same lab, they can share a single timetagger, which provides a convenient shared clock for sifting.

5.2.1 Basis transformations using group velocity dispersion

In spite of the advantages of asymmetric basis switching (discussed in Section 3.3.2), Alice and Bob used 50-50 splitters to switch between the two measurement bases because that was what was available. The FB measurements were implemented using COTS devices based on chirped FBGs (manufactured by Teraxion). The operating principle is the same as that of the Proximion devices described in Section 4.4, but

unlike those devices, the Teraxion devices used in this demonstration apply GVD that is periodic over 50-GHz (0.4 nm) spectral channels matched to the International Telecommunication Union (ITU) grid, i.e., instead of being continuous over the spectral width of the signal and idler photons, the group delay resets every 0.4 nm. The magnitude of the applied group delay slope is $|D| = 600$ ps/0.4 nm.

Fig. 5-7 plots photon coincidences recorded between Alice and Bob's four possible combinations of measurements in the TB and FB, with the SPDC source pumped by a cw laser. If Alice and Bob both record photons in the TB, their photons have correlated arrival times within ~ 110 ps FWHM. This correlation width is dominated by the timing jitter of Alice and Bob's detectors and time-tagging electronics; the correlation time of this SPDC source, as determined by the phase-matching bandwidth, is 2.8 ps. If Alice and Bob measure in different bases, the correlation width is broadened to ~ 630 ps, as expected for these GVD elements. Since the dispersion-broadened photon temporal envelope exceeds the ~ 100 ps timing resolution of the SNSPDs, precise spectral measurements can be made [93]. Lastly, if Alice and Bob both record photons in the FB, they recover a narrow correlation width of 140 ps, exemplifying nonlocal dispersion cancellation [161]. The mismatch between the correlation widths measured with and without dispersion is an input to the excess spectral noise factor, ξ_ω, as described in Section 3.2.

5.2.2 Results

For this EB demonstration, the SPDC source was pumped with pulses with duration 1.49 ns FWHM. This value corresponds to a baseline (i.e., without Eve's interference) frequency correlation of $\sigma_{\omega,0} = 125$ MHz (standard deviation) between Alice and Bob's photons. The nonlocal dispersion cancellation of the FB measurements allowed Alice and Bob to resolve frequency correlations to $\sigma'_\omega = 273$ MHz, giving them an excess spectral noise factor $\xi_\omega = 3.74$. Using this ξ_ω, the Holevo information was bounded to $\chi(A;E) = 1.56$ bpc, including finite-key corrections with security parameter $\varepsilon_s = 10^{-5}$.

The maximum reconciled information was $\beta I(A;B) = 2.39$ bpc, obtained for

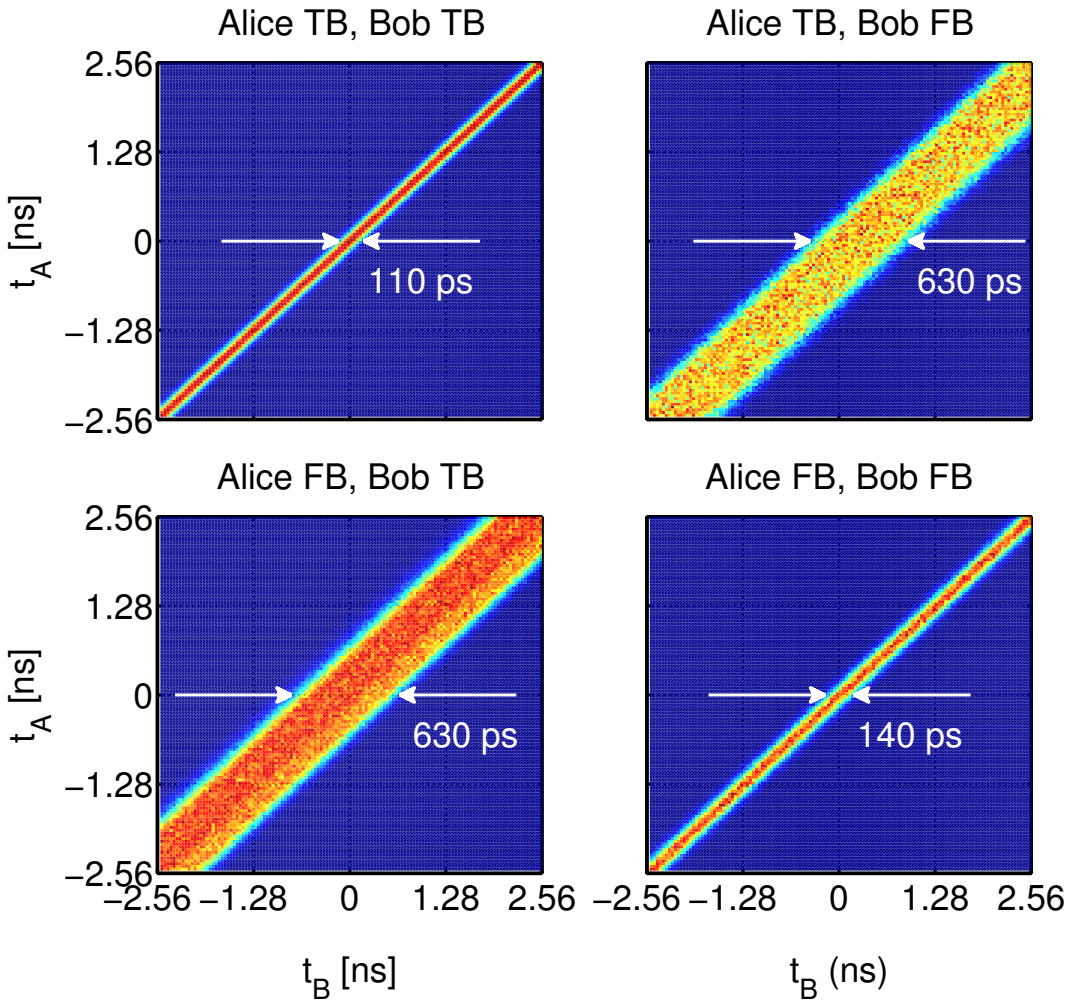

Figure 5-7: Measured two-photon correlations for all combinations of Alice's and Bob's measurement basis choices. When both Alice and Bob use the TB, the measured correlations are limited by SNSPD timing jitter. When only one party uses the FB, the measured correlations are broadened to a duration determined by the applied GVD. When both Alice and Bob use the FB, narrow timing correlations are recovered.

$M = 64$. Errors in the raw keys were reconciled using a multi-layer low-density parity-check (LDPC) code that was specifically designed for high-dimensional QKD applications [1]. The code performs efficient large-alphabet error correction from the least significant to the most significant bit. It is particularly effective at correcting errors caused by timing jitter, which comprise the vast majority of errors in the raw keys. The efficiency β of the error correction code is defined as

$$\beta = \frac{\text{mutual information reconciled by code}}{I(A;B)}, \tag{5.1}$$

where $I(A;B)$ is the mutual information of Alice and Bob's raw keys. The maximum possible mutual information is $\log_2 M$, but in practice $I(A;B)$ is lowered by the effects of detector timing jitter, background counts, and multipair emissions from the SPDC source. Fig. 5-8 plots β obtained by this code as a function of the symbol error rate (SER) for different alphabet sizes $M \in \{16, 32, 64, 128, 256, 512\}$ and a large number of datasets produced by the campus SPDC source.

Finally, to eliminate Eve's information about the reconciled keys, privacy amplification was implemented using hash functions based on multiplication by random Toeplitz matrices [118]. Privacy amplification shortens a reconciled key that is n symbols long to a secure key that is $r < n$ symbols long, where the ratio r/n is given by

$$\frac{r}{n} = \frac{\text{secure PIE}}{\log_2 M}. \tag{5.2}$$

5.2.3 Discussion

In this demonstration, the maximum observed secret-key rate was 456 bps, and the corresponding secure PIE was 0.83 bpc. The sample size was $N \sim 3 \times 10^5$ counts, which is relatively small: the secure PIE was only $\sim 80\%$ of its asymptotic value. The penalty due to finite key lengths, Δ_{FK}, was 0.20 bpc. With only an order-of-magnitude increase in N, we can more than halve the finite-key correction to 0.07 bpc, and when $N \geq 10^8$, $\Delta_{\text{FK}} < 0.01$ bpc. We can easily increase N, and thus, the secure PIE, by using a longer integration time and/or asymmetric basis selection.

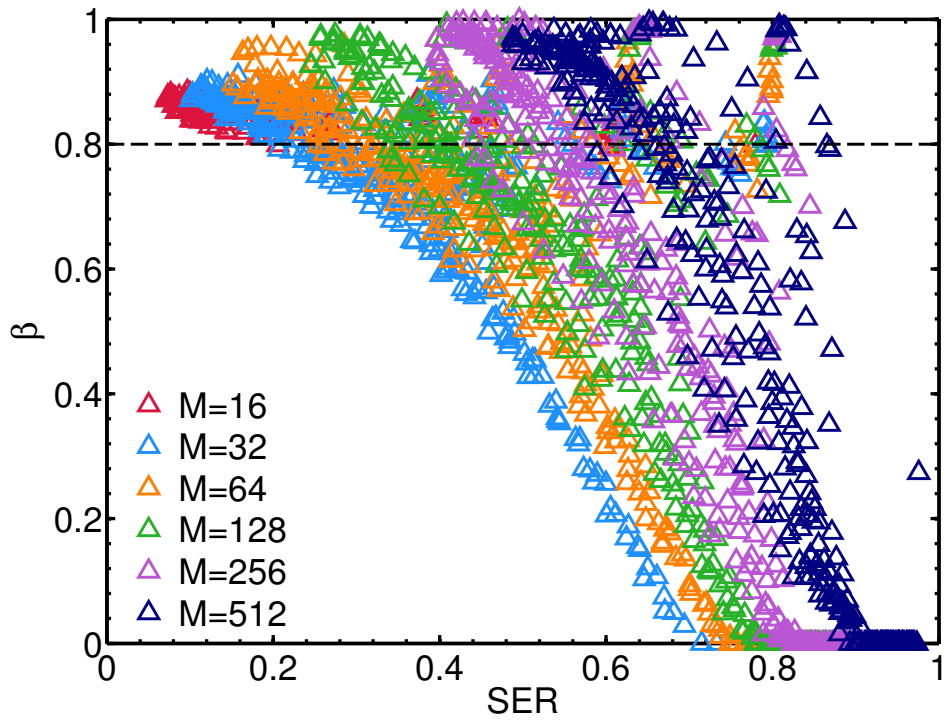

Figure 5-8: Reconciliation efficiency β obtained by the layered LDPC error reconciliation code [1], plotted as a function of the symbol error rate (SER) of the raw keys, for alphabet sizes $M \in \{16, 32, 64, 128, 256, 512\}$.

Another way to raise the secret-key rate is to increase the pump pulse rate while maintaining the SPDC pair generation rate per pulse, i.e., while keeping the peak power constant. In this demonstration, the average SPDC pair generation rate was 0.28 pairs/pulse, and the pump pulse repetition rate was 8.3 MHz. The pulse duty cycle was low, $\sim 1\%$, which leaves substantial room for improvement in the repetition rate.

An alternate strategy is to increase the average entangled pair generation rate by increasing the pump power. However, this also increases the likelihood of producing multiple entangled pairs by a single pulse or during the same symbol. This is similar to the trade-off Alice experiences in P&M QKD when determining the optimal average photon number μ of her attenuated laser transmitter: higher intensities increase her transmission rate but also increase the risk of multi-photon emissions that are susceptible to PNS attacks. The decoy-state method was developed to counter this trade-off [129–131]. Decoy states are also helpful in EB QKD because some security proofs assume a single photon pair is emitted per symbol or per pump pulse [69, 73, 175]. However, there is another issue related to multi-pair emissions that decoy states do not solve.

Multi-pair emissions tend to reduce Alice and Bob's mutual information because independent pairs, even if produced during the same pump pulse, are not correlated with each other. Suppose two photon pairs are produced by a single pulse and that Alice and Bob each detect only one photon, but their detected photons come from different pairs. Then, the sifting algorithm would interpret these detection events as a photon coincidence, but the detected arrival times would be uncorrelated. To exemplify this effect, Fig. 5-9 plots the raw and reconciled mutual information ($I(A;B)$ and $\beta I(A;B)$) for $M = 256$ as functions of the pump power (or equivalently, the entangled pair generation rate per slot). Higher pair generation rates correspond to lower mutual information per photon coincidence. (The data in Fig. 5-9 were recorded using a cw pump for the SPDC source, but the same relationship between pump power and mutual information holds for pulsed pumping.)

The multi-pair emission rate can also be affected by the alphabet size. Photon

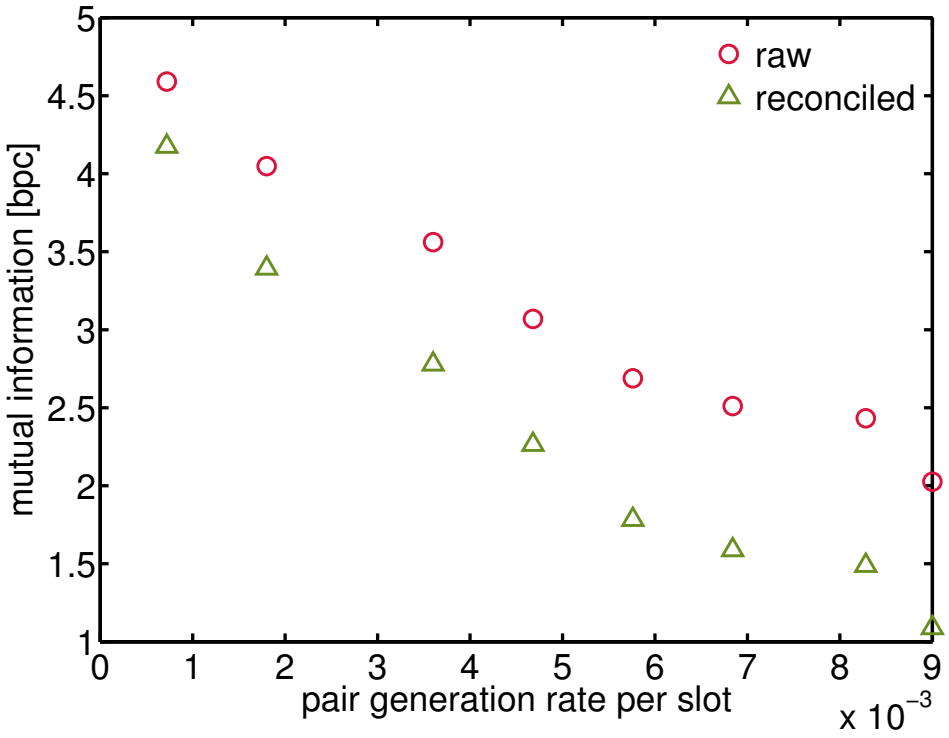

Figure 5-9: Experimentally obtained raw and reconciled mutual information ($I(A;B)$ and $\beta I(A;B)$) for $M = 256$ as functions of the pump power (or equivalently, the entangled pair generation rate per slot).

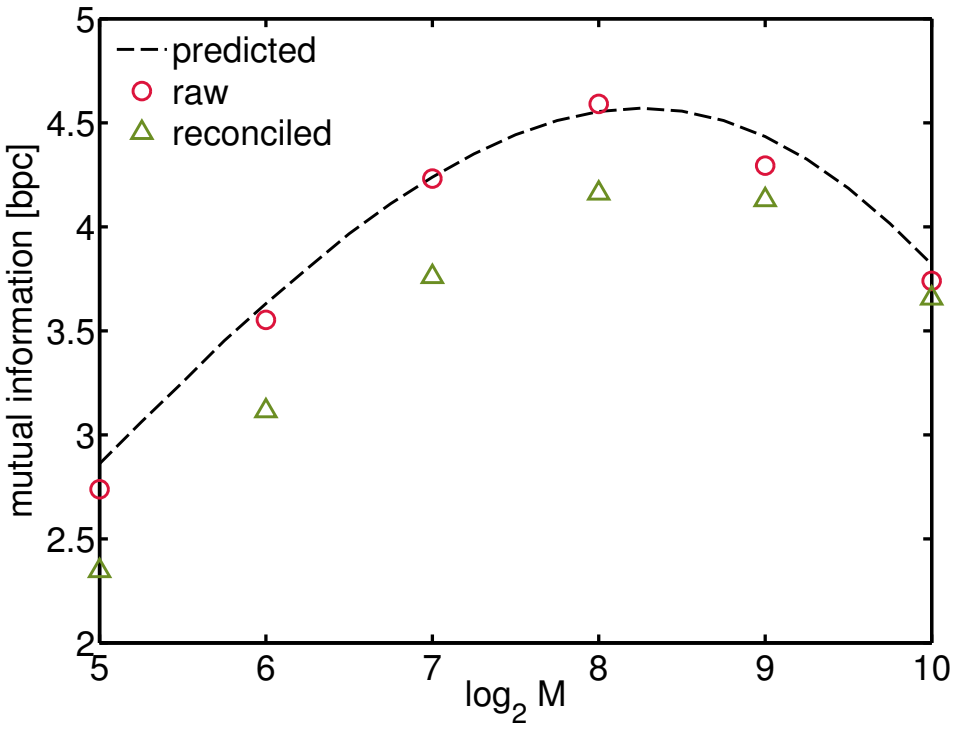

Figure 5-10: Predicted raw mutual information and experimentally obtained raw and reconciled mutual information ($I(A;B)$ and $\beta I(A;B)$) for fixed pump power as functions of $\log_2 M$.

pairs emitted during the same symbol, which has duration $M \times T_{\text{slot}}$, are classified as multi-pairs. For a fixed average pair generation rate per slot, the likelihood of multi-pair emissions increases as M increases. Although a larger alphabet size leads to a larger theoretical maximum mutual information, in practice the mutual information does not increase indefinitely as M increases. This effect is illustrated in Fig. 5-10, which plots the predicted, raw, and reconciled mutual information as functions of $\log_2 M$. The predicted mutual information was computed using a numerical model that considers the effects of multi-pair emissions, loss, background counts, and detector timing jitter on the mutual information.

Finally, there is yet another trade-off to consider, and that is the same one depicted in Fig. 4-1(a): for a fixed slot duration, a larger M leads to a smaller rate of symbols per second.

In summary, higher pump powers lead to higher entangled pair generation rates

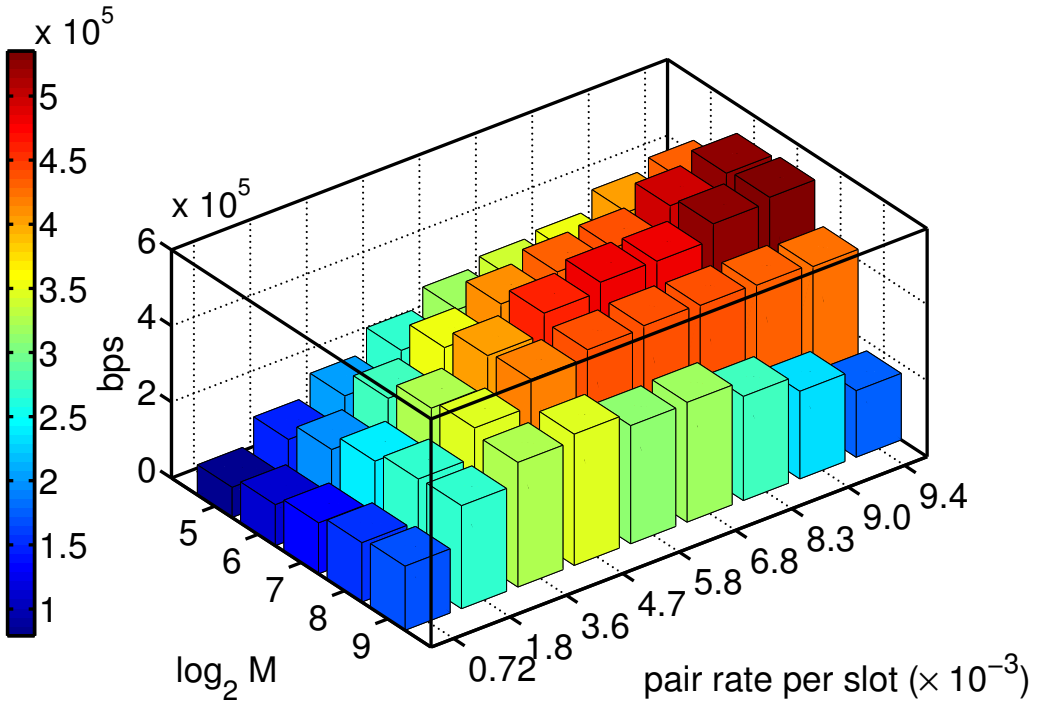

Figure 5-11: Reconciled mutual information rate in bits per second as functions of both the pump power and the alphabet size.

(and thus to higher detected coincidence rates) but also reduce the secure PIE due to the effects of multi-pair emissions on the mutual information. A larger M raises the maximum possible secure PIE, but as M increases, multi-pair emissions eventually cause the secure PIE to decrease, assuming a fixed slot duration. Continuing this assumption, a larger M also corresponds to a lower rate of symbols per second. Fig. 5-11 plots Alice and Bob's reconciled mutual information rate in bits per second as functions of both the pump power and the alphabet size, showing that both pump power and M should not be increased indefinitely if the goal is to obtain higher communication rates. Thus, several experimental parameters can and should be optimized for each use scenario, considering channel loss, receivable photon rates, etc.

We can improve upon this EB DO-QKD demonstration by optimizing these parameters, adding asymmetric basis switching, improving the source-to-detector coupling, and/or updating the pulsed pump source. Most of these strategies affect the

mutual information or the detected coincidence rate, but an as-yet unmentioned approach is targeted at reducing the Holevo information: by increasing D, the magnitude of the GVD. This increases Alice and Bob's spectral resolution. For the same observed value of σ_t, increasing D reduces the corresponding value of σ_ω, which in turn reduces ξ_ω. With this motivation, the Proximion GVD elements, with $|D| = 10,000$ ps/nm, were purchased after the completion of the lab demonstration described in this section, to be used for DO-QKD experiments in the deployed-fiber testbed (including the P&M experiments described in Chapter 4, which chronologically occurred after this demonstration).

5.3 Toward entanglement-based dispersive-optics quantum key distribution over deployed fiber

For EB DO-QKD experiments in the deployed-fiber testbed, we use the LL SPDC source. Alice and the SPDC source are located at LL. The detectors at LL are four quads of NbN SNSPDs, as described in Section 4.4. (Some time after the demonstration of P&M DO-QKD, three additional quads became available.) Not all of the quads have four operational nanowires, but this is not a huge concern because we are also constrained by the number of available timetagging channels. The efficiency per nanowire is between 13-17%, and FWHM timing jitters range from 58-90 ps. Bob is located at MIT. Detectors at MIT are more (different) WSi SNSPDS with detection efficiencies between 65-70% and FWHM timing jitters ranging from 200-290 ps.

5.3.1 Timing synchronization over deployed fiber

There are two significant challenges to counting coincidences between MIT and LL over the deployed fiber. First, it goes without saying (but we'll say it anyway), that when Alice and Bob are located on different ends of the deployed fiber, they can no longer share a timetagger. Instead, Alice and Bob each have a Picoquant Hydraharp. To obtain any useful timing correlations, the two Hydraharps require a

shared frequency reference.

Fig. 5-12 displays results from the first photon coincidence counting measurements over the deployed fiber. The acquisition time was ten seconds for each trial. These initial experiments used a type-0 bulk PPLN SPDC source built by Ben Dixon (since these experiments happened before the LL PPKTP source was built). The upper plot of Fig. 5-12 shows an example of the cross-correlation between signal photons detected at LL and idler photons detected on campus without any shared frequency reference. No dispersion compensation was used; since the signal and idler spectral widths are 13 nm, the expected temporal broadening due to fiber dispersion is 9 ns. However, the correlation peak width is on the order of microseconds, which exceeds the expected width by three orders of magnitude, even when accounting for dispersion. Additionally, the signal-to-noise ratio is very low (or more accurately, the background is unusually high).

In a subsequent test, we optically transmitted a 10 MHz reference signal (using a laser diode and an EOM) from LL to campus to synchronize the frequency references of the two Hydraharps. The lower plot of Fig. 5-12 shows an example of the cross-correlation between signal photons detected at LL and idler photons detected on campus in the presence of this optically shared frequency reference. Both the correlation peak width and the signal-to-noise ratio are the expected order of magnitude.

To maintain a permanent shared frequency reference between LL and campus, identical COTS global positioning system (GPS) receivers were installed at both locations. Each receiver uses timing signals acquired from GPS satellites to discipline an on-board oscillator that in turn drives several reference outputs, including a 10 MHz sine wave. The GPS-derived 10 MHz signals provide frequency references for both Hydraharps. Alice also connects the 10 MHz reference signal to the AWG in SPDC pulsed pump source and to a PPG that outputs periodic pulses. Just as in the P&M DO-QKD experiments, Alice uses the PPG and an EOM to modulate the cw output of a laser diode to produce periodic sync pulses that can be transmitted over the fiber to Bob. Alice also electrically connects the PPG output to her Hydraharp.

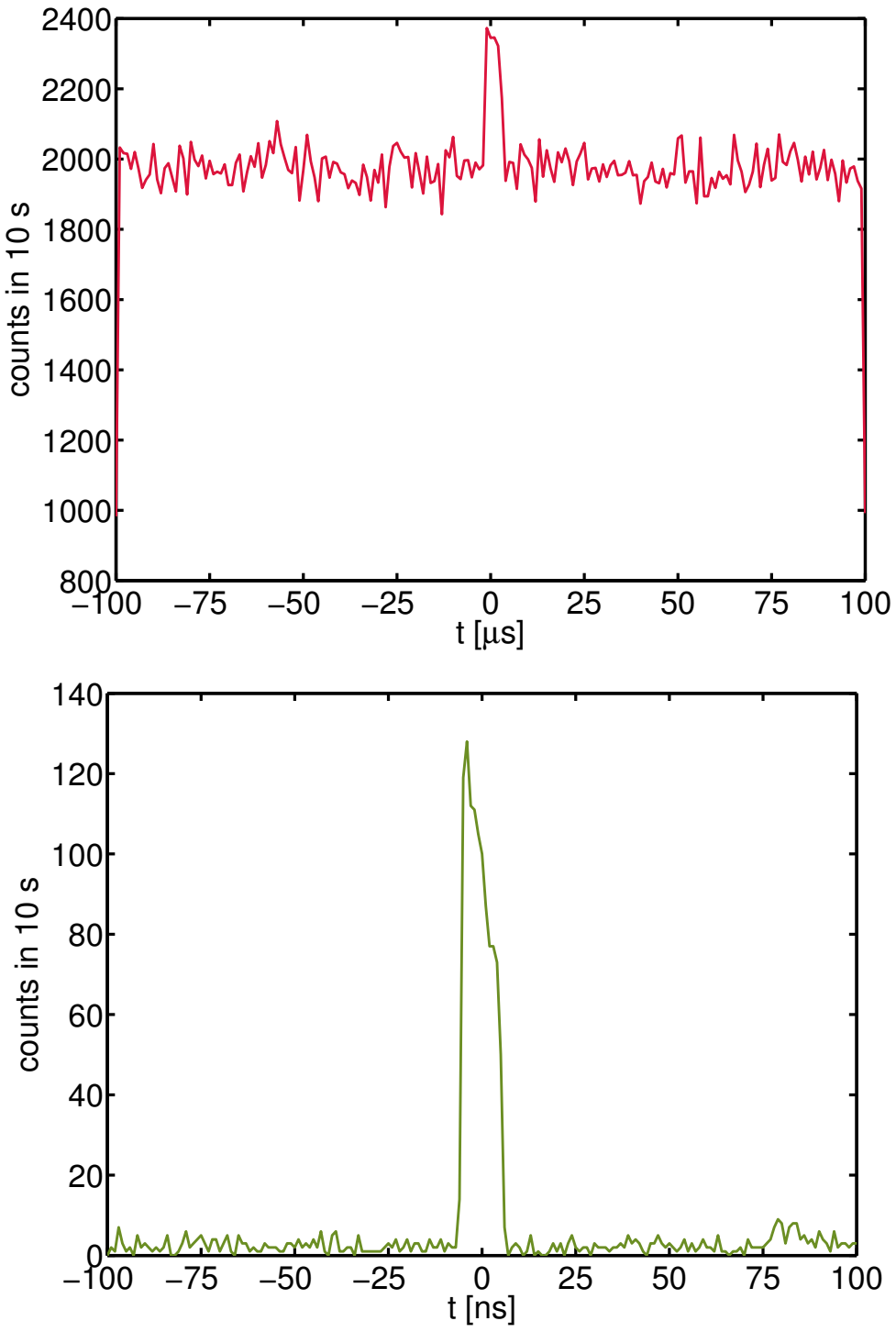

Figure 5-12: Upper: cross-correlation between signal photons detected at LL and idler photons detected on campus without a shared frequency reference between the two timetaggers. Lower: the same cross-correlation when a 10 MHz was optically transmitted over the fiber to synchronize the two timetaggers; all other aspects of the measurement were the same. For each plot, the acquisition time was 10 s.

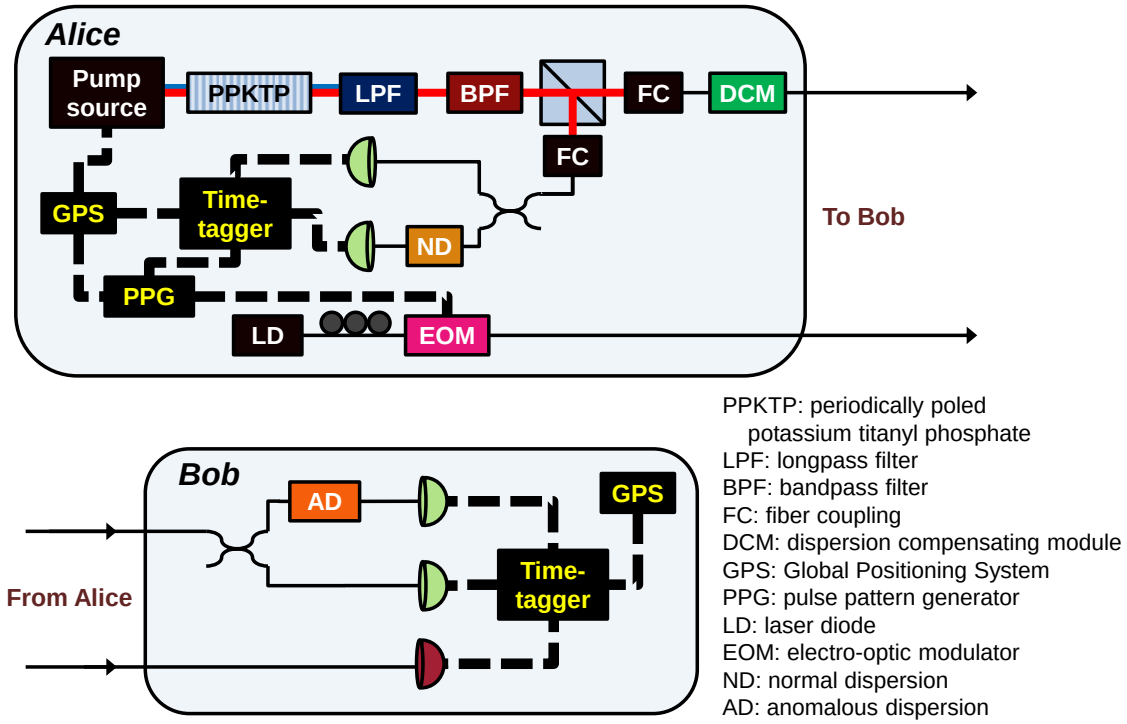

Figure 5-13: Experimental setup for the EB DO-QKD demonstration when using the deployed fiber, including the GPS systems and associated frequency reference connections. The SPDC source is simplified in this illustration. Thin, solid lines indicate optical connections; thick, dashed lines indicate electrical connections; blue lines indicate free-space transmission of the pump beam; and red lines indicate free space transmission of the signal/idler beams.

Fig. 5-13 shows a schematic of the EB DO-QKD setup when using the deployed fiber, including the GPS systems and associated frequency reference connections. Alice pre-compensates for the dispersion of the deployed fiber using a FBG-based dispersion compensating module (DCM); it was recently obtained from Proximion AB and has lower insertion loss than the spool of DCF mentioned in Section 4.4.

The other challenge to coincidence counting over the deployed fiber comes from the fiber itself. Since it is outside the controllable laboratory environment, it is subject to large temperature changes that can cause its effective round-trip length to change by over ten meters in a single day (albeit a day when the outside temperature changed by several tens of degrees Farenheit) [188]. Cross-correlations between photons detected at LL and on campus over intervals of thirty minutes show large drifts of the

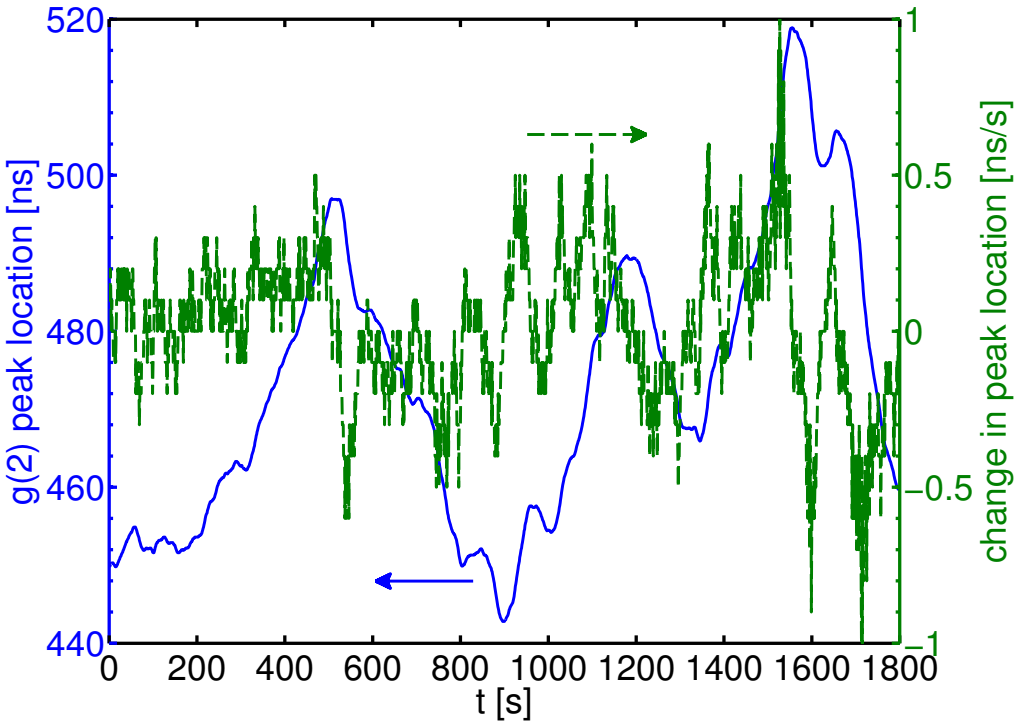

Figure 5-14: Solid curve, left y-axis: temporal location of the peak in the cross-correlation between signal photons detected at LL and idler photons detected on campus, as measured over 30 mins with the cross-correlation computed once per second. Dashed curve, right y-axis: corresponding rate of change of the peak location.

coincidence peak in time. Fig. 5-14 is a representative plot that marks the location of the cross-correlation peak, as well as the rate of change of the peak location, over a thirty-minute acquisition period, when the cross-correlation is computed for each second's worth of data (offline, not in real time).

The peak drift data plotted in Fig. 5-14 show a swing of nearly 80 ns in < 30 minutes. The equivalent length of fiber is ~ 16 m. Although length changes > 10 m have been observed, they usually occur in the presence of large temperature changes over many hours. In contrast, the data in Fig. 5-14 are representative of all of our thirty-minute coincidence counting measurements on a summer day: each thirty-minute integration period showed a swing of several 10s of ns. Using the same photon detection events, Fig. 5-15 plots the cross-correlation for the full 30-min period. Values on the x-axis of Fig. 5-15 correspond to values on the left y-axis of Fig. 5-14. In

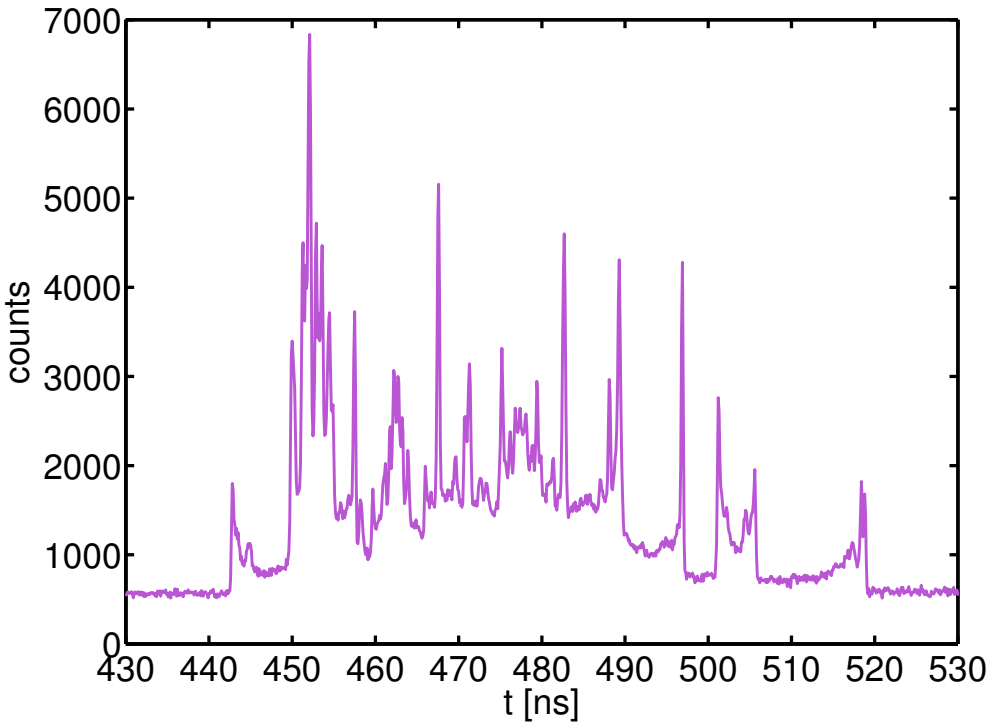

Figure 5-15: Cross-correlation between signal photons detected at LL and idler photons detected on campus for 30 mins with timetaggers synced using GPS-based frequency references.

Fig. 5-15, multiple discrete narrow peaks appear. Based on prior characterization of the fiber link, we expect temperature-induced timing changes to manifest themselves as slow, continuous drifts. Thus, we might expect Fig. 5-15 to contain a single, wide peak corresponding to a continuous change in the deployed fiber length. However, one possible explanation for the discrete peaks seen in Fig. 5-15 is that the rate of fiber drift is not constant, going up to as much as 1 ns/s, as shown on the right y-axis of Fig. 5-14. The times at which no narrow peaks appear in Fig. 5-15 are correlated with high rates of fiber drift. This implies that when the fiber length is changing rapidly, the coincidence rate at a given t is too low to contribute to a statistically significant cross-correlation peak.

Despite this data, we remain unconvinced that length changes > 10 m are truly occurring so rapidly and so frequently. The cause of our skepticism is the fact that GPS-disciplined oscillators provide synchronization only to the order of nanoseconds.

Fig. 5-12 clearly indicates that it is better to have the GPS-based 10 MHz references than to not have them; they reduce the frequency difference between the two timetaggers by several orders of magnitude. In the near future, we will continue to investigate whether the remaining frequency mismatch is affecting the timetagging by testing atomic frequency references at either end of the deployed fiber.

5.3.2 Nonlocal dispersion cancellation over deployed fiber

We cannot estimate the temporal and spectral correlations between Alice's and Bob's detected photons without correcting for the temporal drift of the cross-correlation peak. We need to be able to isolate the correlation peak widths from any artificial broadening or narrowing due to timing drifts. For the current detected coincidence rates (on the order of 100 Hz) and the observed temporal drift, the path length difference between Alice and Bob is not sufficiently stable to acquire enough samples to estimate parameters and minimize the finite-key deductions in the secure PIE.

Although the cause of the observed temporal drift is not yet verified, we can use the out-of-band sync pulses to reclock the detected photon arrival times at both Alice's and Bob's timetaggers. Fig. 5-16 plots the timing correlations for all combinations of basis choices after reclocking. The plots in Fig. 5-16 were produced using the full thirty minutes' worth of data and stand in stark contrast to Fig. 5-15, which corresponds to the Alice TB, Bob TB case without reclocking.

Using the reclocked timetags, we obtain $\xi_\omega \approx 740$ and $\chi(A;E) > 5$ bpc, which is too high to obtain any positive secure PIE. The GVD is not sufficiently cancelled between the TB and FB measurements. Comparing the widths of the correlation peaks in Fig. 5-16, $\sigma_\Delta \equiv \sqrt{\sigma_t^2 - \sigma_{\text{cor}}'^2} = 104$ ps, even when deconvolving out the effects of unequal detector timing jitters (differing by 90 ps FWHM).

Local measurements of dispersion cancellation at LL obtain $\sigma_\Delta = 30$ ps, corresponding to $\xi_\omega \approx 10$ and $\chi(A;E) \approx 2$ bpc. The target value of σ_Δ is on the order of 1 ps. Part of the high σ_Δ can be attributed to the fact that the Proximion GVD elements do not produce group delays that are flat across their ~ 4 nm passbands. Instead, they each have a group delay ripple with magnitude ~ 65 ps/nm^2. The rip-

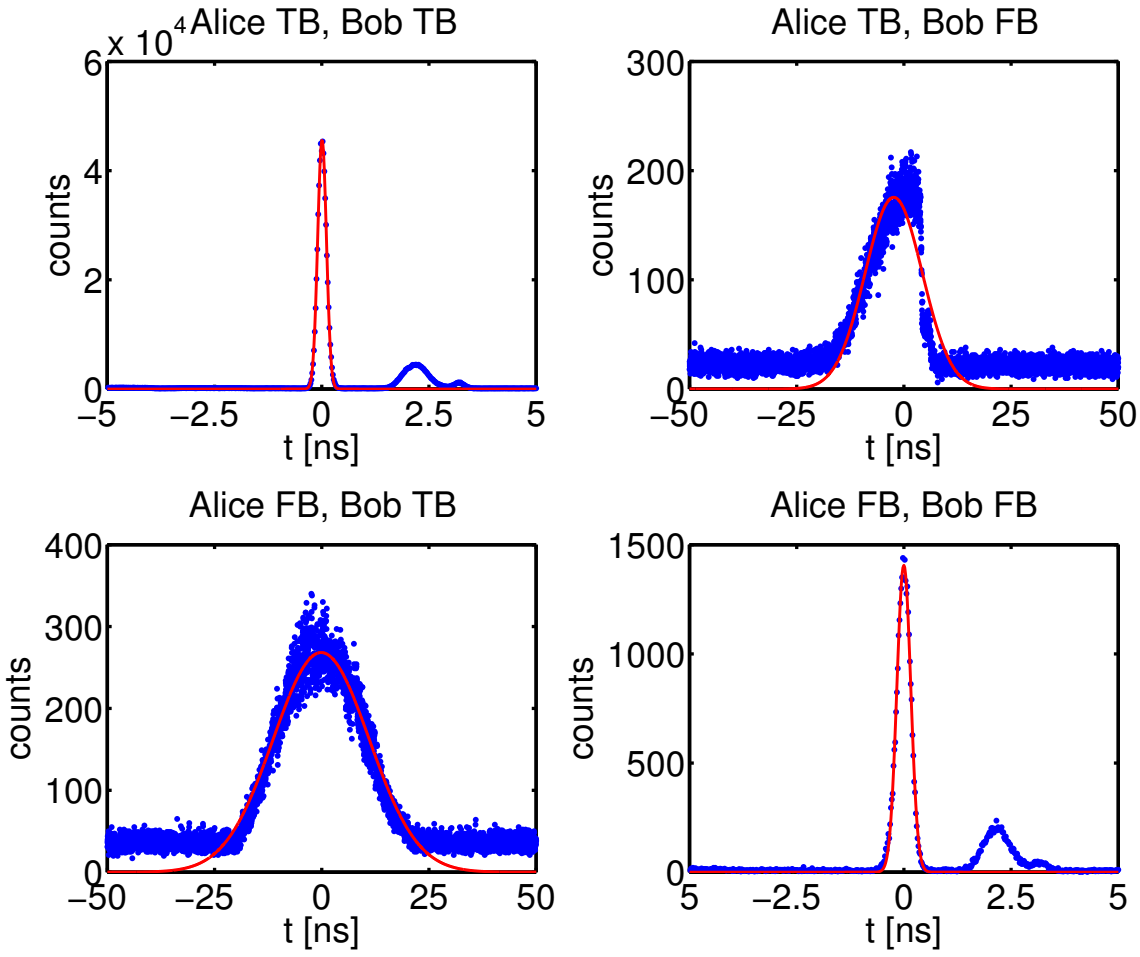

Figure 5-16: Two-photon correlations measured over the deployed fiber for all combinations of Alice's and Bob's measurement basis choices. Blue = measured data; red = Gaussian fits to data. The plots were produced using photon detection events acquired for 30 mins; the detection events were reclocked using the periodic sync pulses recorded by each of Alice's and Bob's timetaggers. In the Alice TB, Bob FB plot, the sharp cutoff around 5 ns appears because the passband of Bob's GVD element cuts off part of the idler spectrum. In the Alice TB, Bob TB and Alice FB, Bob FB plots, the auxiliary peaks around 2 ns appear as an artifact of the reclocking, due to afterpulsing in the periodic sync signal. This can be removed with updates to the algorithm.

M	SER	$I(A;B)$
2	0.0557	0.691
4	0.1420	1.270
8	0.2649	1.613
16	0.3429	2.052
32	0.4079	2.515

Table 5.1: Raw key results for reclocked photon detection events measured over the deployed fiber.

ple contributes to mismatch in the normal and anomalous GVD applied by Alice and Bob. By filtering the signal and idler, we reduce the spectral width over which the GVD ripple has an effect. After filtering to around 0.5 nm FWHM, with the filters' center wavelengths set to maximize the detected coincidence rate, σ_Δ is reduced to 22.7 ps, which exceeds the target value by an order of magnitude but is also less than one-fourth of the value obtained over the deployed fiber. In the future, we will continue to investigate whether the fiber, the timetaggers, or the reclocking are affecting the measured timing correlation widths and σ_Δ.

5.3.3 Mutual information over deployed fiber

Table 5.1 summarizes the raw key results obtained using the reclocked photon detection events. The reported values of $I(A;B)$ were computed directly from the raw keys and do not include error reconciliation. With these results, no secure PIE is obtained.

5.3.4 Further work

To obtain a positive secure PIE over the deployed fiber, we need to improve the nonlocal cancellation of GVD to reduce ξ_ω. This could be aided by filtering the signal and idler photons, at the expense of the coincidence rate, or by using a programmable waveshaper to implement a custom group delay to offset the ripple in the Proximion elements. We could even replace our GVD elements with ones that have a larger value of $|D|$, which allows us to tolerate a larger temporal mismatch in the GVD

cancellation. We also need to ascertain whether the GPS-based frequency references are affecting the timing correlations between the photons detected by Alice and Bob.

An alternate strategy to combat fiber drift is to integrate the DO-QKD setup with the LL fiber stabilization system described in Ref. [188]. The LL system can achieve sub-wavelength stabilization of the round-trip fiber length. With some modifications, it should be adaptable for one-way stabilization. However, in its current state, the stabilization system introduces an overwhelming amount of spontaneous Raman scattering into the SPDC spectral channel. In the near future, the system will be adapted to reduce the scattering.

Chapter 6

High-dimensional Einstein-Podolsky-Rosen steering

In this chapter, we introduce Einstein-Podolsky-Rosen (EPR) steering and describe how it can be observed using the EB DO-QKD setup, both in the lab and over the deployed fiber.

6.1 Introduction to Einstein-Podolsky-Rosen steering

EPR steering (or steerability) is a form of quantum correlation that lies between entanglement and Bell nonlocality [189–191]. Entanglement, or equivalently, nonseparability, refers to the fact that the composite state $|\Psi\rangle$ of two particles A and B cannot be written as the tensor product of the single-particle states $|\psi_A\rangle$ and $|\psi_B\rangle$:

$$|\Psi\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle, \tag{6.1}$$

while a separable state can. Bell nonlocality rules out the existence of local hidden variable models that describe reality [135, 192] and is the strongest type of quantum correlation [189].

Steering is a type of correlation that is strictly stronger than entanglement and

strictly weaker than Bell nonlocality [189, 190]. That is, all states that demonstrate steerability are also entangled/nonseparable, but not all nonseparable states are steerable. Similarly, all states that violate a Bell inequality are steerable (and also entangled/nonseparable), but not all steerable states demonstrate Bell nonlocality [193]. Interestingly, entanglement and Bell nonlocality are both symmetric between Alice and Bob, but steering is inherently asymmetric [189].

Steering can be defined as a task: Alice prepares a bipartite quantum state, sends half of it to Bob, and measures her own half. By measuring her system, Alice can remotely steer Bob's system. She cannot deterministically prepare Bob's system in a desired state (that would be superluminal signaling), but if she sends her measurement results to Bob, Bob can measure his own system and check that his conditional states have been steered [192]. After a sufficiently large number of repetitions, Bob can estimate the strength of the correlations between his system and Alice's [192]. The goal is for Alice to convince Bob that she can prepare entangled states and steer Bob's system. The alternative is that Bob's system is described by some local hidden state model [189]. A local hidden state model is the steering analogue of a local hidden variable model in Bell tests.

Like Bell tests, steering experiments also have loopholes, but they are easier to close than those of Bell tests. In particular, the detection efficiency required to close the detection loophole is lower than the threshold for Bell tests [192, 194], and in fact, the required efficiency can be made arbitrarily low [195]. As a result, loophole-free steering experiments [196] were achieved years before loophole-free Bell tests [137, 138, 197].

The asymmetry of the steering task implies that Bob must trust both quantum mechanics and his own measurements but need not trust Alice, her measurements, or the entanglement source [191]. This asymmetric trust allows for one-sided device-independent QKD (1SDI-QKD) [198, 199], where the security is tied to the violation of an EPR steering inequality. Practically, 1SDI-QKD broadens the scope of possible scenarios for QKD; for example, it is well-suited to scenarios when Bob is in a fixed, secure location but Alice may be roaming in an untrusted region.

Because it is experimentally easier to violate a steering inequality than a Bell inequality, it is also easier to implement 1SDI-QKD than fully DI QKD. For 1SDI-QKD, the detection loophole must be closed, but as previously stated, the required efficiency is lower than that for fully DI QKD [192, 198]. Additionally, the locality and freedom-of-choice loopholes become irrelevant, since security proofs already assume that no information can leak out of Alice's or Bob's labs unless they allow it [195].

Because steering is strictly stronger than entanglement, the violation of an EPR steering inequality over some channel indicates that the channel preserves entanglement. We can use the EB DO-QKD setup and the same TB and FB measurements to test a high-dimensional EPR steering inequality over the deployed fiber, thereby confirming that we can distribute time-energy entanglement from LL to MIT. Time-energy entanglement is commonly verified using a Franson interferometer setup [88]. However, if we used a Franson interferometer to test for entanglement over the deployed fiber, we would have to stabilize two separate interferometers located on opposite ends of the deployed fiber. This would require us to build a new real-time feedback system. By testing steering instead of Franson interference, we can demonstrate entanglement distribution without needing interferometric stability or real-time feedback.

6.2 Steering inequality for continous variables using discretized measurements

The photons produced by the SPDC source are entangled in time and frequency, which are continuous degrees of freedom. Ref. [200] introduces an EPR steering inequality for continuous variables that relies on discretized measurements:

$$H(T_B|T_A) + H(\Omega_B|\Omega_A) \geq \log_2\left(\frac{\pi e}{\Delta t_B \Delta\omega_B}\right). \tag{6.2}$$

We define the steering parameter, S, as the left-hand side (LHS) of this inequality: $S \equiv H(T_B|T_A) + H(\Omega_B|\Omega_A)$. Here, $H(T_B|T_A)$ is the discrete Shannon entropy of

measurements of the arrival time of Bob's photon conditioned on measurements of the arrival time of Alice's photon. We assume that the range of possible arrival times, denoted T_f, is broken up into M discrete time slots of duration Δt_B; thus, $T_f = M \times \Delta t_B$. Similarly, $H(\Omega_B|\Omega_A)$ is the discrete Shannon entropy of measurements of the frequency of Bob's photon conditioned on measurements of the frequency of Alice's photon. We assume that the frequency is measured with resolution $\Delta\omega_B$. We note that (6.2) explicitly depends on the resolution of Bob's measurements only. We assume that Alice and Bob use the same measurement settings with temporal resolution $\Delta t = \Delta t_B$ and frequency resolution $\Delta\omega = \Delta\omega_B$.

Using the dispersive FB measurements, the frequency resolution $\Delta\omega$ is related to the temporal resolution Δt by

$$\Delta\omega = \frac{2\pi c}{\lambda^2}\frac{\Delta t}{D}, \tag{6.3}$$

where λ is the photon wavelength and D is the magnitude of the applied GVD in units of ps/nm. In our experiment, $\lambda \sim 1560$ nm and $D \sim 10{,}000$ ps/nm. We assume that there are M discrete frequency slots of width Δ_ω, and thus the range of possible frequencies is $\Omega_f = M \times \Delta_\omega$.

The analysis of the timetagged photon detection events follows the same sifting procedure used for DO-QKD and illustrated in Fig. 3-2. Only the raw keys are used to verify EPR steering. From the raw keys, we build up $M \times M$ joint probability matrices for each of the two measurement bases: $P_T(T_A, T_B)$ and $P_\Omega(\Omega_A, \Omega_B)$. For example, $p_T(a, b)$, the entry in the ath row and bth column of P_T, is the probability that using the TB, Alice detected her photon in the ath slot and Bob detected his in the bth slot:

$$p_T(a, b) = \frac{N_T(a, b)}{N_{TB}}, \tag{6.4}$$

where $N_T(a, b)$ is the number of instances when Alice detected her photon in the ath slot and Bob detected his in the bth slot, and N_{TB} is the total number of coincidences detected using the TB. Similarly, $p_\Omega(a, b)$, the entry in the ath row and bth column of P_Ω, is the probability that using the FB, Alice detected her photon in the ath slot

and Bob detected his in the bth slot, and

$$p_\Omega(a,b) = \frac{N_\Omega(a,b)}{N_{FB}}, \tag{6.5}$$

where $N_\Omega(a,b)$ and N_{FB} are the FB analogues to $N_T(a,b)$ and N_{TB}, respectively. Using the joint probability matrices, we can compute all relevant entropies to obtain the steering parameter, S. Without loss of generality, we define the entropies and write all further calculations using only the TB; the results are the same for the FB.

$$\begin{aligned} H(T_B|T_A) &= H(T_A,T_B) - H(T_A) && (6.6)\\ H(T_A,T_B) &= -\sum_{a,b} p_T(a,b)\log_2 p_T(a,b) && (6.7)\\ H(T_A) &= -\sum_{a} p_T(a)\log_2 p_T(a), && (6.8) \end{aligned}$$

where

$$p_T(a) = \sum_b p_T(a,b). \tag{6.9}$$

We also compute δS, the uncertainty in S, by assuming that coincidence counts follow Poissonian statistics. The uncertainty in number of counts $N_T(a,b)$ for a given matrix entry is assumed to be $\delta N_T(a,b) = \sqrt{N_T(a,b)}$. This uncertainty is propagated through the probability and entropy calculations[1].

6.3 Results and discussion

Fig. 6-1 plots the steering parameter as measured both locally at LL and over the deployed fiber for $M \in \{2,4,8\}$ and $20 \leq \Delta t \leq 350$ ps. The right-hand side (RHS) of (6.2) is also plotted as a solid black curve. Violations of the steering inequality (6.2) occur in the region under this curve. The size of the error bars is δS.

[1] I think I'll work on LaTeX-ing the propagation of uncertainties in an appendix: use $\delta N_T(a,b)$ and Eq. (6.4) to get $\delta p(a,b)$; use $\delta p(a,b)$ and the entropy formulas to get $\delta H(T_A,T_B)$ and $\delta H(T_A)$; etc.

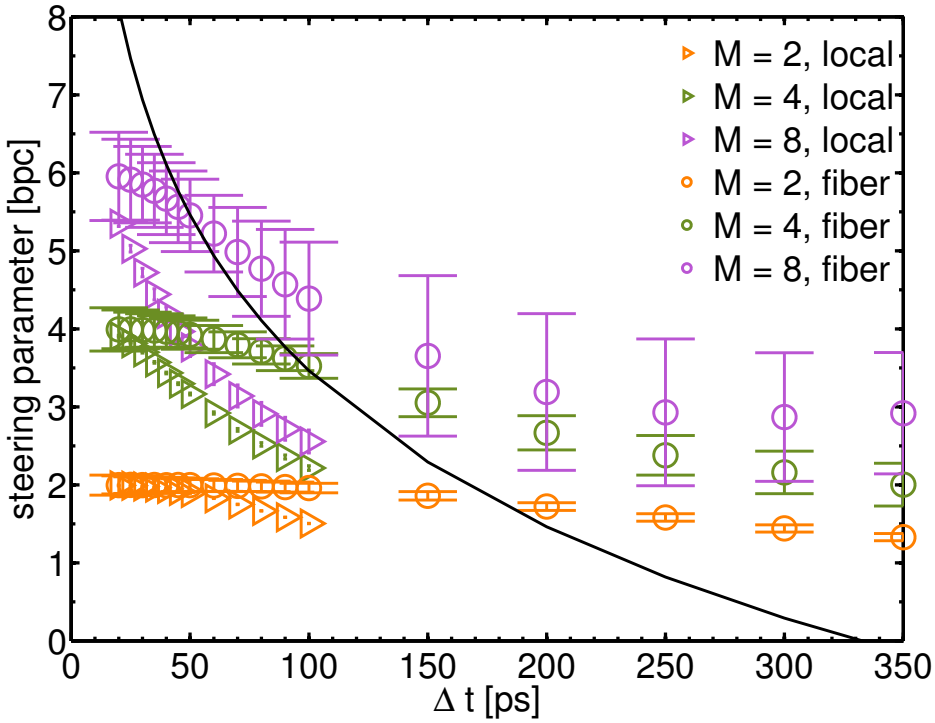

Figure 6-1: Steering parameter, S, as a function of Δt for alphabet size $M \in \{2, 4, 8\}$, measured locally at LL and over the deployed fiber. The black solid curve indicates the value of the RHS of (6.2). Points under this curve indicate violations of the steering inequality.

We define the degree of violation as the quantity

$$\log_2\left(\frac{\pi e}{\Delta t_B \Delta\omega_B}\right) - S(M, \Delta t_B), \tag{6.10}$$

i.e., the RHS of (6.2) minus the LHS of (6.2), where a positive value indicates that (6.2) is violated. Here, $S(M, \Delta t_B)$ denotes the value of the steering parameter for a particular choice of M and $\Delta t = \Delta t_B$ (with $\Delta\omega_B \propto \Delta t_B$). The values of M and Δt_B both directly affect the degree of violation. For example, the degree of violation increases as Δt decreases because this directly makes the RHS of (6.2) bigger. However, decreasing Δt also indirectly affects S because the temporal resolution affects the entropy calculations; decreasing Δt also indirectly causes S to increase, but this is offset by larger increase in the RHS of (6.2).

The degree of violation also increases as M decreases because this directly makes S smaller. However, it is undesirable to make M arbitrarily small because this also decreases the mutual information between Alice and Bob. Fig. 6-2 plots the raw mutual information obtained for $M = 4$ in each basis, locally at LL and over the deployed fiber. In theory, $I(A; B)$ should be the same for each basis; in our experiments, the mutual information obtained in the FB is lower due to the imperfect dispersion cancellation of the Proximion GVD elements, as described in Section 5.3.2. The imperfect dispersion cancellation broadens the correlation peak width, which reduces the mutual information. For the experiment over the deployed fiber, the mutual information in the FB is significantly lower than that of the TB because the timing jitter of the FB SNSPD on campus was ~ 90 ps greater than that of the TB SNSPD, which also broadens the correlation peak width and reduces the mutual information. No steps were taken to correct for this difference in timing jitter.

Fig. 6-2 shows that $I(A; B)$ is minimal for small Δt, where the degree of violation is greatest. We assume that applications of this EPR steering inequality will take advantage of its high-dimensional nature, i.e., its ability to show steerability while also exchanging a large amount of mutual information per detected photon coincidence [201]. Therefore, a high degree of violation alone is not necessarily satisfactory; we

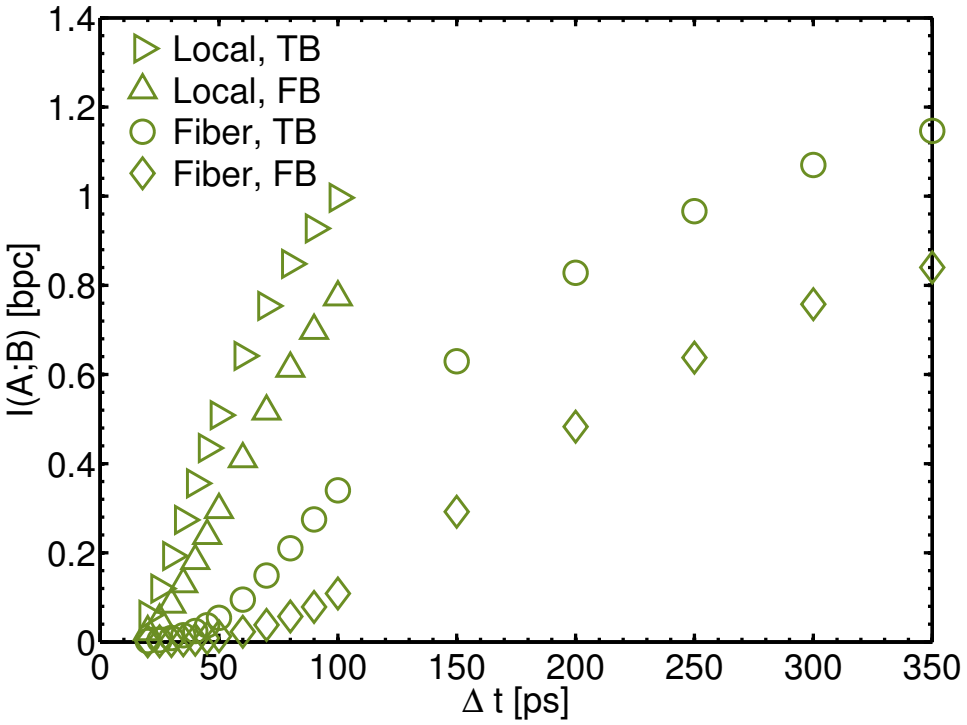

Figure 6-2: Alice and Bob's mutual information, $I(A;B)$, as a function of Δt, measured in both bases locally at LL and over the deployed fiber. Small values of Δt are correlated with small values of $I(A;B)$ but also with high degrees of violation of (6.2).

		Local				Fiber			
M	Δt (ps)	Degree of violation	δS	$I(A;B)$ in TB	$I(A;B)$ in FB	Degree of violation	δS	$I(A;B)$ in TB	$I(A;B)$ in FB
2	25	5.473	0.005	0.007	0.003	5.463	0.116	0.000	0.000
	50	3.567	0.004	0.074	0.030	3.466	0.083	0.002	0.000
	100	1.958	0.118	0.310	0.184	1.503	0.061	0.033	0.006
4	25	3.647	0.012	0.120	0.048	3.469	0.249	0.004	0.001
	50	2.298	0.013	0.509	0.297	1.538	0.185	0.054	0.013
	100	1.247	0.118	0.996	0.774	-0.062	0.158	0.340	0.109
8	25	2.435	0.043	0.594	0.338	1.550	0.519	0.061	0.017
	50	1.700	0.118	1.266	0.942	0.008	0.463	0.388	0.123
	100	0.906	0.147	1.845	1.587	-0.925	0.724	1.023	0.552

Table 6.1: Steering results for selected values of Δt, highlighting the tradeoff between degree of violation and mutual information.

would like to violate the steering inequality with sufficient confidence (in this case, a situation-dependent number of standard deviations), while also achieving high mutual information. Table 6.1 lists the degree of violation as defined in (6.10), δS, and mutual information in both bases, obtained locally and over the deployed fiber, for some combinations of M and Δt_B, reiterating the trade-off between high degree of violation and high mutual information.

To our knowledge, this is the first demonstrated violation of a high-dimensional EPR steering inequality over a deployed fiber, and possibly the first violation of any steering inequality over a deployed fiber. We note that when using our dispersion-based frequency measurements with $|D| = 10,000$ ps/nm, the RHS of (6.2) constrains $\Delta t_B \leq 330$ ps, as can by seen from the solid curve in Fig. 6-1. This implies the need for high-resolution single-photon detectors, which have only become widely available at telecom wavelengths in the past few years.

By violating the high-dimensional EPR steering inequality in the lab and over the deployed fiber, we confirm that our SPDC source produces pairs of entangled photons[2] and that we can successfully distribute entanglement over the fiber link.

[2]Performing QKD experiments does not necessarily confirm the presence of entanglement. QKD does not explicitly require entangled photons but does require that the channel is not entanglement-breaking [23].

This marks an important milestone in the development of our Boston-area quantum network.

Chapter 7

Summary and outlook

We described DO-QKD and its first security proof, which shows asymptotic security against the class of arbitrary collective attacks [2]. As part of this thesis, we extended the security proof to show that DO-QKD still provides security against collective attacks even in the realistic regime of finite-length keys [72]. Assuming achievable parameters, we numerically showed that DO-QKD obtains $> 90\%$ of the asymptotic secure PIE for an experimentally feasible number of detected coincidences, $N \approx 10^7$, with performance on par with other single-photon QKD protocols.

We then described the P&M implementation of DO-QKD, including demonstrations both in the lab and over our newly developed, 42-km deployed-fiber testbed running between MIT and MITLL. By the combined advantages of high-dimensional encoding and fast single-photon detectors, we achieved record secret-key rates for each channel loss tested [76].

We then described the EB implementation of DO-QKD, including the construction of multiple SPDC sources, the first demonstration in the lab [71], and steps toward demonstrating DO-QKD over the deployed fiber. We then noted that the same EB DO-QKD setup could be used to violate an EPR steering inequality without requiring interferometric stability or real-time feedback. Since steering is a type of quantum correlation that is strictly stronger than entanglement, a violation of a steering inequality is also a proof of entanglement. We violated a high-dimensional EPR steering inequality in the lab and over the deployed fiber, confirming that our

SPDC source produces pairs of entangled photons and that we can successfully distribute the entanglement over the fiber link. In doing so, we have performed the first demonstration of the violation of a high-dimensional EPR steering inequality over a deployed fiber.

The deployed-fiber experiments require further investigation related to timing accuracy, which we expect will only improve upon the results presented here. To successfully demonstrate EB DO-QKD over the deployed fiber, we will also have to improve the nonlocal dispersion cancellation. We note that Ref. [73] is an updated security proof for DO-QKD that holds against general attacks, albeit with more pessimistic secret-key rates, compared to the proofs presented here, and it would be useful to use that proof to analyze our current or future data. We also plan to integrate the EB DO-QKD setup with the LL fiber stabilization system described in Ref. [188], pending some modifications relating to reducing noise caused by that system.

Ultimately, we have demonstrated both the utility of high-dimensional QKD and the feasibility of our testbed for further applications in quantum communication and networking.

Appendix A

Timing correlations after applying dispersion

In this appendix, we mathematically verify the relationship between σ_t, the two-photon correlation time after applying GVD, and σ_ω, the spectral correlation between Alice and Bob's detected photons.

We start by writing the original two-photon correlation time, assuming a non-specific biphoton state, as

$$\sigma_{\text{cor}}^2 = \int dtdu(t-u)^2 \langle \hat{E}_S^\dagger(t)\hat{E}_I^\dagger(u)\hat{E}_I(u)\hat{E}_S(t)\rangle. \tag{A.1}$$

When applying equal and opposite GVD with magnitude D, the field operators are described in the frequency domain as

$$\hat{E}_S(t) = \int \frac{d\omega}{2\pi}\hat{A}_S(\omega)e^{-i\omega t}e^{iD\omega^2/2} \tag{A.2}$$

$$\hat{E}_I(t) = \int \frac{d\omega}{2\pi}\hat{A}_I(\omega)e^{-i\omega t}e^{-iD\omega^2/2}, \tag{A.3}$$

where ω is defined as the detuning from $\omega_p/2$, and ω_p is the pump frequency of the SPDC source. The phase $\propto \omega^2$ is due to the GVD. Subscripts S denote the signal photon and I denote the idler photon.

Using these field operators, the two-photon correlation time after Alice applies

normal GVD and Bob applies anomalous GVD is then

$$\begin{aligned}\sigma_t^2 = \int dtdu \frac{d\omega d\xi d\omega' d\xi'}{(2\pi)^4}(t-u)^2 \langle \hat{A}_S^\dagger(\omega')\hat{A}_I^\dagger(\xi')\hat{A}_I(\xi)\hat{A}_S(\omega)\rangle \\ \times \exp\left[it(\omega'-\omega) + iu(\xi'-\xi) + \frac{iD(\omega^2-\xi^2-\omega'^2+\xi'^2)}{2}\right].\end{aligned} \tag{A.4}$$

We make a change of variables $t_\pm \equiv t \pm u$ and obtain

$$\begin{aligned}\sigma_t^2 = \frac{1}{2}\int dt_+ dt_- \frac{d\omega d\xi d\omega' d\xi'}{(2\pi)^4} t_-^2 \langle \hat{A}_S^\dagger(\omega')\hat{A}_I^\dagger(\xi')\hat{A}_I(\xi)\hat{A}_S(\omega)\rangle \\ \times \exp\left[\frac{i(\omega'-\omega)(t_+ + t_-) + i(\xi'-\xi)(t_+ - t_-)}{2}\right] \\ \times \exp\left[\frac{iD(\omega^2-\xi^2-\omega'^2+\xi'^2)}{2}\right].\end{aligned} \tag{A.5}$$

Then we define $\omega_\pm \equiv \omega \pm \omega'$ and $\xi_\pm \equiv \xi \pm \xi'$, resulting in

$$\begin{aligned}\sigma_t^2 = \frac{1}{2}\left(\frac{1}{4}\right)\int dt_+ dt_- \frac{d\omega_+ d\omega_- d\xi_+ d\xi_-}{(2\pi)^4} t_-^2 \\ \times \left\langle \hat{A}_S^\dagger\left(\frac{\omega_+ - \omega_-}{2}\right)\hat{A}_I^\dagger\left(\frac{\xi_+ - \xi_-}{2}\right)\hat{A}_I\left(\frac{\xi_+ + \xi_-}{2}\right)\hat{A}_S\left(\frac{\omega_+ + \omega_-}{2}\right)\right\rangle \\ \times \exp\left[\frac{it_+(-\omega_- - \xi_-)}{2} + \frac{it_-(\xi_- - \omega_-)}{2} + \frac{iD(\omega + \omega_- - \xi_+\xi_-)}{2}\right].\end{aligned} \tag{A.6}$$

We use

$$\frac{1}{2}\int dt_+ \exp\left[\frac{it_+}{2}(-\omega_- - \xi_-)\right] = 2\pi\delta(\omega_- + \xi_-) \tag{A.7}$$

to obtain

$$\begin{aligned}\sigma_t^2 = \frac{1}{4}\int dt_- \frac{d\omega_+ d\omega_- d\xi_+ d\xi_-}{(2\pi)^4} t_-^2 \\ \times \left\langle \hat{A}_S^\dagger\left(\frac{\omega_+ - \omega_-}{2}\right)\hat{A}_I^\dagger\left(\frac{\xi_+ - \xi_-}{2}\right)\hat{A}_I\left(\frac{\xi_+ + \xi_-}{2}\right)\hat{A}_S\left(\frac{\omega_+ + \omega_-}{2}\right)\right\rangle \\ \times 2\pi\delta(\omega_- + \xi_-)\exp\left[\frac{it_-(\xi_- - \omega_-)}{2} + \frac{iD(\omega_+\omega_- - \xi_+\xi_-)}{2}\right].\end{aligned} \tag{A.8}$$

After carrying out the integral over ξ_-, we obtain

$$\sigma_t^2 = \frac{1}{4}\int dt_- \frac{d\omega_+ d\omega_- d\xi_+}{(2\pi)^3} t_-^2 \times \left\langle \hat{A}_S^\dagger\left(\frac{\omega_+ - \omega_-}{2}\right)\hat{A}_I^\dagger\left(\frac{\xi_+ - \omega_-}{2}\right)\hat{A}_I\left(\frac{\xi_+ + \omega_-}{2}\right)\hat{A}_S\left(\frac{\omega_+ + \omega_-}{2}\right)\right\rangle \times \exp\left[it_-\omega_- + \frac{iD\omega_-(\omega_+ + \xi_+)}{2}\right]. \tag{A.9}$$

We will use

$$\int dt_- t_-^2 e^{-it_-\omega_-} = -2\pi \frac{d^2}{d(\omega_-)^2}\delta(\omega_-), \tag{A.10}$$

so to solve Eq. (A.9), we must integrate by parts twice. Doing so, we obtain

$$\sigma_t^2 = -\frac{2\pi}{4}\int \frac{d\omega_+ d\omega_- d\xi_+}{(2\pi)^3}\delta(\omega_-) \times \frac{d^2}{d(\omega_-)^2}\left(\left\langle \hat{A}_S^\dagger\left(\frac{\omega_+ - \omega_-}{2}\right)\hat{A}_I^\dagger\left(\frac{\xi_+ - \omega_-}{2}\right)\hat{A}_I\left(\frac{\xi_+ + \omega_-}{2}\right)\hat{A}_S\left(\frac{\omega_+ + \omega_-}{2}\right)\right\rangle \times \exp\left[\frac{iD\omega_-(\omega_+ + \xi_+)}{2}\right]\right). \tag{A.11}$$

To differentiate the expectation value in Eq. (A.11), we rewrite the operators as

$$\hat{A}(\omega) = \int dt \hat{E}(t) e^{i\omega t}. \tag{A.12}$$

After differentiating twice with respect to ω_-, we obtain

$$\begin{aligned}\sigma_t^2 = -\frac{2\pi}{4}\int \frac{d\omega_+ d\omega_- d\xi_+}{(2\pi)^3} dt du dt' du' \langle \hat{E}_S^\dagger(t')\hat{E}_I^\dagger(u')\hat{E}_I(u)\hat{E}_S(t)\rangle \delta(\omega_-) \\ \times \exp\left[\frac{i\omega_+}{2}(t-t') + \frac{i\xi_+}{2}(u-u')\right] \\ \times \exp\left[\frac{i\omega_-}{2}(t+t'-(u+u')) + \frac{iD\omega_-(\omega_+ + \xi_+)}{2}\right] \\ \times \left(-\frac{1}{4}\left(t+t'-(u+u')\right)^2 - \frac{D^2}{4}(\omega_+ + \xi_+)^2 \right. \\ \left. +2\frac{i}{2}\left(t+t'-(u+u')\right)\frac{iD}{2}(\omega_+ + \xi_+)\right).\end{aligned} \tag{A.13}$$

After integrating over ω_-, we obtain

$$\begin{aligned}\sigma_t^2 = -\frac{1}{4}\int \frac{d\omega_+ d\xi_+}{(2\pi)^2} dt du dt' du' \\ \times \langle \hat{E}_S^\dagger(t')\hat{E}_I^\dagger(u')\hat{E}_I(u)\hat{E}_S(t)\rangle \exp\left[\frac{i\omega_+}{2}(t-t') + \frac{i\xi_+}{2}(u-u')\right] \\ \times \left(-\frac{1}{4}\left(t+t'-(u+u')\right)^2 - \frac{D^2}{4}(\omega_+ + \xi_+)^2 \right. \\ \left. +2\frac{i}{2}\left(t+t'-(u+u')\right)\frac{iD}{2}(\omega_+ + \xi_+)\right).\end{aligned} \tag{A.14}$$

For notational ease, we divide σ_t^2 into three terms, $\sigma_t^2 \equiv X_1 + X_2 + X_3$, where

$$\begin{aligned}X_1 = \frac{1}{4}\int \frac{d\omega_+ d\xi_+}{(2\pi)^2} dt du dt' du' \langle \hat{E}_S^\dagger(t')\hat{E}_I^\dagger(u')\hat{E}_I(u)\hat{E}_S(t)\rangle \\ \times \exp\left[\frac{i\omega_+}{2}(t-t') + \frac{i\xi_+}{2}(u-u')\right]\left(\frac{1}{4}\left(t+t'-(u+u')\right)^2\right),\end{aligned} \tag{A.15}$$

$$\begin{aligned}X_2 = \frac{1}{4}\int \frac{d\omega_+ d\xi_+}{(2\pi)^2} dt du dt' du' \langle \hat{E}_S^\dagger(t')\hat{E}_I^\dagger(u')\hat{E}_I(u)\hat{E}_S(t)\rangle \\ \times \exp\left[\frac{i\omega_+}{2}(t-t') + \frac{i\xi_+}{2}(u-u')\right]\left(\frac{D^2}{4}(\omega_+ + \xi_+)^2\right),\end{aligned} \tag{A.16}$$

and

$$X_3 = \frac{1}{4}\int \frac{d\omega_+ d\xi_+}{(2\pi)^2} dt du dt' du' \langle \hat{E}_S^\dagger(t')\hat{E}_I^\dagger(u')\hat{E}_I(u)\hat{E}_S(t)\rangle \\ \times \exp\left[\frac{i\omega_+}{2}(t-t') + \frac{i\xi_+}{2}(u-u')\right] \\ \times \left(\frac{D}{2}\left(t+t'-(u+u')\right)(\omega_+ + \xi_+)\right). \tag{A.17}$$

It can be easily shown by integrating over ω_+ and ξ_+ that X_1 simplifies to

$$X_1 = \int dt du (t-u)^2 \langle \hat{E}_S^\dagger(t)\hat{E}_I^\dagger(u)\hat{E}_I(u)\hat{E}_S(t)\rangle \\ = \sigma_{\text{cor}}^2. \tag{A.18}$$

We will show a few more steps of the simplification of X_2, starting with

$$X_2 = \frac{1}{2}\left(\frac{D^2}{4}\right)\int \frac{d\omega_+}{2\pi} dt du dt' \langle \hat{E}_S^\dagger(t')\hat{E}_I^\dagger(u)\hat{E}_I(u)\hat{E}_S(t)\rangle \exp\left[\frac{i\omega_+}{2}(t-t')\right]\omega_+^2 \\ + \frac{1}{2}\left(\frac{D^2}{4}\right)\int \frac{d\xi_+}{2\pi} dt du du' \langle \hat{E}_S^\dagger(t)\hat{E}_I^\dagger(u')\hat{E}_I(u)\hat{E}_S(t)\rangle \exp\left[\frac{i\xi_+}{2}(u-u')\right]\xi_+^2 \\ + \frac{1}{2}\left(\frac{D^2}{4}\right)\int \frac{d\omega_+ d\xi_+}{(2\pi)^2} dt du dt' du' \langle \hat{E}_S^\dagger(t')\hat{E}_I^\dagger(u')\hat{E}_I(u)\hat{E}_S(t)\rangle \\ \times \exp\left[\frac{i\omega_+}{2}(t-t') + \frac{i\xi_+}{2}(u-u')\right]\omega_+\xi_+. \tag{A.19}$$

After integration by parts and using Eq. (A.12) to rewrite the operators, we obtain

$$X_2 = -D^2 \int dt du dt' \frac{d\omega d\xi d\omega' d\xi'}{(2\pi)^4} \langle \hat{A}_S^\dagger(\omega')\hat{A}_I^\dagger(\xi')\hat{A}_I(\xi)\hat{A}_S(\omega)\rangle \delta(t-t') \\ \times \frac{d^2}{dt'^2}\left(\exp[i\omega' t' + iu(\xi'-\xi) - i\omega t]\right) \\ - D^2 \int dt du du' \frac{d\omega d\xi d\omega' d\xi'}{(2\pi)^4} \langle \hat{A}_S^\dagger(\omega')\hat{A}_I^\dagger(\xi')\hat{A}_I(\xi)\hat{A}_S(\omega)\rangle \delta(u-u') \\ \times \frac{d^2}{du'^2}\left(\exp[it(\omega-\omega') + iu'\xi' - iu\xi]\right) \\ - 2D^2 \int dt du dt' du' \frac{d\omega d\xi d\omega' d\xi'}{(2\pi)^4} \langle \hat{A}_S^\dagger(\omega')\hat{A}_I^\dagger(\xi')\hat{A}_I(\xi)\hat{A}_S(\omega)\rangle \\ \times \delta(t-t')\delta(u-u')\frac{d}{dt'}\frac{d}{du'}\left(\exp[i\omega' t' + i\xi' u' - iu\xi - i\omega t]\right). \tag{A.20}$$

After taking the derivatives and integrating over the δ-functions, we obtain

$$\begin{aligned} X_2 = -D^2 \int dt du \frac{d\omega d\xi d\omega' d\xi'}{(2\pi)^4} \langle \hat{A}_S^\dagger(\omega') \hat{A}_I^\dagger(\xi') \hat{A}_I(\xi) \hat{A}_S(\omega) \rangle \\ \times (-\omega'^2 - \xi'^2 - 2\omega'\xi') \exp[it(\omega' - \omega) + iu(\xi' - \xi)]. \end{aligned} \tag{A.21}$$

After simplifying more δ-functions, we obtain

$$\begin{aligned} X_2 &= D^2 \int \frac{d\omega d\xi}{(2\pi)^2} \langle \hat{A}_S^\dagger(\omega) \hat{A}_I^\dagger(\xi) \hat{A}_I(\xi) \hat{A}_S(\omega) \rangle (\omega + \xi)^2 \\ &= D^2 \sigma_\omega^2. \end{aligned} \tag{A.22}$$

It turns out that X_3 is the tricky term, since it contains one power of time and one power of frequency. X_3 has the form $f(x) = \int dx x \exp[i\alpha x]$, which does not converge, but its Cauchy principal value is zero, and thus we can simplify the integral as $X_3 = 0$.

Therefore, σ_t, the two-photon correlation time after applying GVD is related to σ_ω by by $\sigma_t^2 = \sigma_{\text{cor}}^2 + D^2 \sigma_\omega^2$.

Bibliography

[1] Zhou, H., Wang, L. & Wornell, G. Layered schemes for large-alphabet secret key distribution. In *Proc. Information Theory and Applications Workshop (ITA), 2013*, 1–10 (IEEE, Piscataway, NJ, 2013).

[2] Mower, J. *et al.* High-dimensional quantum key distribution using dispersive optics. *Phys. Rev. A* **87**, 062322 (2013).

[3] Comandar, L. C. *et al.* Room temperature single-photon detectors for high bit rate quantum key distribution. *Appl. Phys. Lett.* **104**, 021101 (2014).

[4] Zhong, T. *et al.* Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding. *New J. Phys.* **17**, 022002 (2015).

[5] Comandar, L. C. *et al.* Quantum cryptography without detector vulnerabilities using optically-seeded lasers. *Nat. Photon.* **10**, 312–315 (2016).

[6] Huang, D., Huang, P., Lin, D. & Zeng, G. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* **6**, 19201 (2016).

[7] Treiber, A. *et al.* A fully automated entanglement-based quantum cryptography system for telecom fiber networks. *New J. Phys.* **11**, 045013 (2009).

[8] Korzh, B. *et al.* Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat. Photon.* **9**, 163–168 (2015).

[9] Feamster, N., Balakrishnan, H., Rexford, J., Shaikh, A. & van der Merwe, J. The Case for Separating Routing from Routers. In *Proceedings of the ACM SIGCOMM Workshop on Future Directions in Network Architecture*, FDNA '04, 5–12 (ACM, New York, NY, USA, 2004).

[10] Arnbak, A. & Goldberg, S. Loopholes for Circumventing the Constitution: Unrestricted Bulk Surveillance on Americans by Collecting Network Traffic Abroad. *Mich. Telecomm. & Tech. L. Rev.* **21**, 317–361 (2014). `http://repository.law.umich.edu/mttlr/vol21/iss2/3`.

[11] Rogaway, P. The Moral Character of Cryptographic Work. Cryptology ePrint Archive, Report 2015/1162 (2015). `http://eprint.iacr.org/2015/1162`.

[12] Diffie, W. & Hellman, M. New directions in cryptography. *Information Theory, IEEE Transactions on* **22**, 644–654 (1976).

[13] Rivest, R. L., Shamir, A. & Adleman, L. M. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* **21**, 120–126 (1978).

[14] Miller, V. S. *Use of Elliptic Curves in Cryptography*, 417–426 (Springer Berlin Heidelberg, Berlin, Heidelberg, 1986).

[15] Koblitz, N. Elliptic curve cryptosystems. *Mathematics of Computation* **48**, 203–209 (1987).

[16] Campagna, M. *et al.* Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges. ETSI White Paper No. 8 (2015).

[17] Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing* **26**, 1484–1509 (1997).

[18] Lenstra, A. K., Lenstra, H. W., Manasse, M. S. & Pollard, J. M. *The number field sieve*, 11–42 (Springer Berlin Heidelberg, Berlin, Heidelberg, 1993).

[19] Smolin, J. A., Smith, G. & Vargo, A. Oversimplifying quantum factoring. *Nature (London)* **499**, 163–165 (2013).

[20] Mosca, M. Cybersecurity in an era with quantum computers: will we be ready? Cryptology ePrint Archive, Report 2015/1075 (2015). `http://eprint.iacr.org/2015/1075`.

[21] Bernstein, D. J., Buchmann, J. & Dahmen, E. *Post-quantum cryptography* (Springer Science & Business Media, 2009).

[22] Chen, L. *et al.* Report on Post-Quantum Cryptography. National Institute of Standards and Technology Internal Report 8105 (2016).

[23] Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).

[24] Renner, R. Security of quantum key distribution. *Int. J. Quantum Inform.* **6**, 1–127 (2008).

[25] Vernam, G. S. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *J. Am. Inst. Electr. Eng.* **45**, 109–115 (1926).

[26] Shannon, C. E. Communication theory of secrecy systems. *The Bell System Technical Journal* **28**, 656–715 (1949).

[27] Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (Wiley, Indianapolis, IN, 1996), 2 edn.

[28] Paterson, K. G., Piper, F. & Schack, R. Quantum cryptography: a practical information security perspective. In Zukowski, M., Kilin, S. & Kowalik, J. (eds.) *Quantum Communication and Security*, Proceedings, NATO Advanced Research Workshop, 175–180 (IOS Press, Amsterdam, 2007).

[29] Bennett, C. H., Bessete, F., Brassard, G., Salvail, L. & Smolin, J. Experimental quantum cryptography. *Journal of Cryptology* **5**, 3–28 (1992).

[30] Wegman, M. N. & Carter, J. L. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences* **22**, 265–279 (1981).

[31] Bennett, C. H. & Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, 175–179 (IEEE, New York, 1984).

[32] Scarani, V. & Kurtsiefer, C. The black paper of quantum cryptography: Real implementation problems. *Theoretical Computer Science* **560**, 27–32 (2014).

[33] Jain, N. *et al.* Attacks on practical quantum key distribution systems (and how to prevent them). *Contemporary Physics* **57**, 366–387 (2016).

[34] Stebila, D., Mosca, M. & Lütkenhaus, N. *The Case for Quantum Key Distribution*, 283–296 (Springer Berlin Heidelberg, Berlin, Heidelberg, 2010).

[35] Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).

[36] Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **68**, 557–559 (1992).

[37] Barreiro, J. T., Langford, N. K., Peters, N. A. & Kwiat, P. G. Generation of Hyperentangled Photon Pairs. *Phys. Rev. Lett.* **95**, 260501 (2005).

[38] Kaszlikowski, D., Gnaciński, P., Żukowski, M., Miklaszewski, W. & Zeilinger, A. Violations of Local Realism by Two Entangled N-Dimensional Systems Are Stronger than for Two Qubits. *Phys. Rev. Lett.* **85**, 4418–4421 (2000).

[39] Durt, T., Kaszlikowski, D. & Żukowski, M. Violations of local realism with quantum systems described by N -dimensional Hilbert spaces up to $N = 16$. *Phys. Rev. A* **64**, 024101 (2001).

[40] Collins, D., Gisin, N., Linden, N., Massar, S. & Popescu, S. Bell Inequalities for Arbitrarily High-Dimensional Systems. *Phys. Rev. Lett.* **88**, 040404 (2002).

[41] Vértesi, T., Pironio, S. & Brunner, N. Closing the Detection Loophole in Bell Experiments Using Qudits. *Phys. Rev. Lett.* **104**, 060401 (2010).

[42] Dada, A. C., Leach, J., Buller, G. S., Padgett, M. J. & Andersson, E. Experimental high-dimensional two-photon entanglement and violations of generalized Bell inequalities. *Nat. Phys.* **7**, 677–680 (2011).

[43] Nowierski, S. J., Oza, N. N., Kumar, P. & Kanter, G. S. Tomographic reconstruction of time-bin-entangled qudits. *Phys. Rev. A* **94**, 042328 (2016).

[44] Massar, S. Nonlocality, closing the detection loophole, and communication complexity. *Phys. Rev. A* **65**, 032121 (2002).

[45] Goyal, S. K. *et al.* Qudit-Teleportation for photons with linear optics. *Sci. Rep.* **4**, 4543 (2014).

[46] Časlav Brukner, Żukowski, M. & Zeilinger, A. Quantum Communication Complexity Protocol with Two Entangled Qutrits. *Phys. Rev. Lett.* **89**, 197901 (2002).

[47] Časlav Brukner, Żukowski, M., Pan, J.-W. & Zeilinger, A. Bell's Inequalities and Quantum Communication Complexity. *Phys. Rev. Lett.* **92**, 127901 (2004).

[48] Lanyon, B. P. *et al.* Simplifying quantum logic using higher-dimensional Hilbert spaces. *Nat. Phys.* **5**, 134–140 (2009).

[49] Muralidharan, S., Zou, C.-L., Li, L., Wen, J. & Jiang, L. Overcoming erasure errors with multilevel systems. *New J. Phys.* **19**, 013026 (2017).

[50] Fickler, R. *et al.* Quantum Entanglement of High Angular Momenta. *Science* **338**, 640–643 (2012).

[51] Ali Khan, I. & Howell, J. C. Experimental demonstration of high two-photon time-energy entanglement. *Phys. Rev. A* **73**, 031801 (2006).

[52] Ali-Khan, I., Broadbent, C. J. & Howell, J. C. Large-Alphabet Quantum Key Distribution Using Energy-Time Entangled Bipartite States. *Phys. Rev. Lett.* **98**, 060503 (2007).

[53] Durt, T., Cerf, N. J., Gisin, N. & Żukowski, M. Security of quantum key distribution with entangled qutrits. *Phys. Rev. A* **67**, 012311 (2003).

[54] Durt, T., Kaszlikowski, D., Chen, J.-L. & Kwek, L. C. Security of quantum key distributions with entangled qudits. *Phys. Rev. A* **69**, 032313 (2004).

[55] Cerf, N. J., Bourennane, M., Karlsson, A. & Gisin, N. Security of Quantum Key Distribution Using d-Level Systems. *Phys. Rev. Lett.* **88**, 127902 (2002).

[56] Bechmann-Pasquinucci, H. & Tittel, W. Quantum cryptography using larger alphabets. *Phys. Rev. A* **61**, 062308 (2000).

[57] Grover, L. K. A Fast Quantum Mechanical Algorithm For Database Search. In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, 212–219 (ACM, New York, NY, USA, 1996).

[58] Choi, I. *et al.* Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber. *Opt. Express* **22**, 23121–23128 (2014).

[59] Lucamarini, M. *et al.* Efficient decoy-state quantum key distribution with quantified security. *Opt. Express* **21**, 24550–24565 (2013).

[60] Walborn, S. P., Lemelle, D. S., Almeida, M. P. & Ribeiro, P. H. S. Quantum Key Distribution with Higher-Order Alphabets Using Spatially Encoded Qudits. *Phys. Rev. Lett.* **96**, 090501 (2006).

[61] Zhang, L., Silberhorn, C. & Walmsley, I. A. Secure Quantum Key Distribution using Continuous Variables of Single Photons. *Phys. Rev. Lett.* **100**, 110504 (2008).

[62] Etcheverry, S. *et al.* Quantum key distribution session with 16-dimensional photonic states. *Sci. Rep.* **3**, 2316 (2013).

[63] Cañas, G. *et al.* High-dimensional decoy-state quantum key distribution over 0.3 km of multicore telecommunication optical fibers. *arXiv:1610.01682 [quant-ph]* (2016).

[64] Ding, Y. *et al.* High-Dimensional Quantum Key Distribution based on Multicore Fiber using Silicon Photonic Integrated Circuits. *npj Quantum Information* **3**, 25 (2017).

[65] Tittel, W., Brendel, J., Zbinden, H. & Gisin, N. Quantum Cryptography Using Entangled Photons in Energy-Time Bell States. *Phys. Rev. Lett.* **84**, 4737–4740 (2000).

[66] Qi, B. Single-photon continuous-variable quantum key distribution based on the energy-time uncertainty relation. *Opt. Lett.* **31**, 2795–2797 (2006).

[67] Nunn, J. *et al.* Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion. *Opt. Express* **21**, 15959–15973 (2013).

[68] Brougham, T., Barnett, S. M., McCusker, K. T., Kwiat, P. G. & Gauthier, D. J. Security of high-dimensional quantum key distribution protocols using Franson interferometers. *J. Phys. B: At. Mol. Opt. Phys.* **46**, 104010 (2013).

[69] Zhang, Z., Mower, J., Englund, D., Wong, F. N. C. & Shapiro, J. H. Unconditional Security of Time-Energy Entanglement Quantum Key Distribution Using Dual-Basis Interferometry. *Phys. Rev. Lett.* **112**, 120506 (2014).

[70] Brougham, T. & Barnett, S. M. Cavity-enabled high-dimensional quantum key distribution. *J. Phys. B: At. Mol. Opt. Phys.* **47**, 155501 (2014).

[71] Lee, C. *et al.* Entanglement-based quantum communication secured by nonlocal dispersion cancellation. *Phys. Rev. A* **90**, 062331 (2014).

[72] Lee, C., Mower, J., Zhang, Z., Shapiro, J. & Englund, D. Finite-key analysis of high-dimensional time–energy entanglement-based quantum key distribution. *Quantum Inf. Process.* **14**, 1005–1015 (2015).

[73] Niu, M. Y., Xu, F., Shapiro, J. H. & Furrer, F. Finite-key analysis for time-energy high-dimensional quantum key distribution. *Phys. Rev. A* **94**, 052323 (2016).

[74] Walk, N., Barrett, J. & Nunn, J. Composably secure time-frequency quantum key distribution. *arXiv:1609.09436 [quant-ph]* (2016).

[75] Islam, N. T. *et al.* Robust and Stable Delay Interferometers with Application to d-Dimensional Time-Frequency Quantum Key Distribution. *Phys. Rev. Applied* **7**, 044010 (2017).

[76] Lee, C. *et al.* High-rate field demonstration of large-alphabet quantum key distribution. *arXiv:1611.01139 [quant-ph]* (2016).

[77] Gröblacher, S., Jennewein, T., Vaziri, A., Weihs, G. & Zeilinger, A. Experimental quantum cryptography with qutrits. *New J. Phys.* **8**, 75 (2006).

[78] Mafu, M. *et al.* Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Phys. Rev. A* **88**, 032305 (2013).

[79] Mirhosseini, M. *et al.* High-dimensional quantum cryptography with twisted light. *New J. Phys.* **17**, 033033 (2015).

[80] Takesue, H. & Inoue, K. Generation of $1.5-\mu$m band time-bin entanglement using spontaneous fiber four-wave mixing and planar light-wave circuit interferometers. *Phys. Rev. A* **72**, 041804 (2005).

[81] Takesue, H. Long-distance distribution of time-bin entanglement generated in a cooled fiber. *Opt. Express* **14**, 3453–3460 (2006).

[82] Dyer, S. D., Baek, B. & Nam, S. W. High-brightness, low-noise, all-fiber photon pair source. *Opt. Express* **17**, 10290–10297 (2009).

[83] Kues, M. *et al.* On-chip generation of high-dimensional entangled quantum states and their coherent control. *Nature (London)* **546**, 622–626 (2017).

[84] Tanzilli, S. *et al.* PPLN waveguide for quantum communication. *Eur. Phys. J. D* **18**, 155–160 (2002).

[85] Zhong, T., Wong, F. N., Roberts, T. D. & Battle, P. High performance photon-pair source based on a fiber-coupled periodically poled $KTiOPO_4$ waveguide. *Opt. Express* **17**, 12019–12030 (2009).

[86] Zhong, T., Wong, F. N. C., Restelli, A. & Bienfang, J. C. Efficient single-spatial-mode periodically-poled $KTiOPO_4$ waveguide source for high-dimensional entanglement-based quantum key distribution. *Opt. Express* **20**, 26868–26877 (2012).

[87] Kwiat, P. G. *et al.* New High-Intensity Source of Polarization-Entangled Photon Pairs. *Phys. Rev. Lett.* **75**, 4337–4341 (1995).

[88] Franson, J. D. Bell inequality for position and time. *Phys. Rev. Lett.* **62**, 2205–2208 (1989).

[89] Thew, R. T., Nemoto, K., White, A. G. & Munro, W. J. Qudit quantum-state tomography. *Phys. Rev. A* **66**, 012303 (2002).

[90] Thew, R. T., Acín, A., Zbinden, H. & Gisin, N. Bell-Type Test of Energy-Time Entangled Qutrits. *Phys. Rev. Lett.* **93**, 010503 (2004).

[91] Ikuta, T. & Takesue, H. Implementation of quantum state tomography for time-bin qudits. *New J. Phys.* **19**, 013039 (2017).

[92] Takesue, H., Inoue, K., Tadanaga, O., Nishida, Y. & Asobe, M. Generation of pulsed polarization-entangled photon pairs in a $1.55-\mu$m band with a periodically poled lithium niobate waveguide and an orthogonal polarization delay circuit. *Opt. Lett.* **30**, 293–295 (2005).

[93] Avenhaus, M., Eckstein, A., Mosley, P. J. & Silberhorn, C. Fiber-assisted single-photon spectrograph. *Opt. Lett.* **34**, 2873–2875 (2009).

[94] Bennett, C. V. & Kolner, B. H. Upconversion time microscope demonstrating $103\times$ magnification of femtosecond waveforms. *Opt. Lett.* **24**, 783–785 (1999).

[95] Peng, C.-Z. *et al.* Experimental Free-Space Distribution of Entangled Photon Pairs Over 13 km: Towards Satellite-Based Global Quantum Communication. *Phys. Rev. Lett.* **94**, 150501 (2005).

[96] Schmitt-Manderbach, T. *et al.* Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. *Phys. Rev. Lett.* **98**, 010504 (2007).

[97] Erven, C., Couteau, C., Laflamme, R. & Weihs, G. Entangled quantum key distribution over two free-space optical links. *Opt. Express* **16**, 16840–16853 (2008).

[98] Peloso, M. P., Gerhardt, I., Ho, C., Lamas-Linares, A. & Kurtsiefer, C. Daylight operation of a free space, entanglement-based quantum key distribution system. *New J. Phys.* **11**, 045007 (2009).

[99] Wang, J.-Y. *et al.* Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nat. Photon.* **7**, 387–393 (2013).

[100] Cao, Y. *et al.* Entanglement-based quantum key distribution with biased basis choice via free space. *Opt. Express* **21**, 27260–27268 (2013).

[101] Bourgoin, J.-P. *et al.* Free-space quantum key distribution to a moving receiver. *Opt. Express* **23**, 33437–33447 (2015).

[102] Liao, S.-K. *et al.* Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nat. Photon.* **11**, 509–513 (2017).

[103] Elliott, C. *et al.* Current status of the DARPA Quantum Network. *arXiv:quant-ph/0503058* (2005).

[104] Yuan, Z. & Shields, A. Continuous operation of a one-way quantum key distribution system over installed telecom fibre. *Opt. Express* **13**, 660–665 (2005).

[105] Tanaka, A. *et al.* Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization. *Opt. Express* **16**, 11354–11360 (2008).

[106] Peev, M. *et al.* The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **11**, 075001 (2009).

[107] Stucki, D. *et al.* Continuous high speed coherent one-way quantum key distribution. *Opt. Express* **17**, 13326–13334 (2009).

[108] Chen, T.-Y. *et al.* Metropolitan all-pass and inter-city quantum communication network. *Opt. Express* **18**, 27217–27225 (2010).

[109] Stucki, D. *et al.* Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New J. Phys.* **13**, 123001 (2011).

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

[111] Wang, S. *et al.* Field and long-term demonstration of a wide area quantum key distribution network. *Opt. Express* **22**, 21739–21756 (2014).

[112] Dixon, A. R. *et al.* High speed prototype quantum key distribution system and long term field trial. *Opt. Express* **23**, 7583–7592 (2015).

[113] Bunandar, D. *et al.* Metropolitan quantum key distribution with silicon photonics. *arXiv:1708.00434 [quant-ph]* (2017).

[114] Sit, A. *et al.* High-dimensional intracity quantum cryptography with structured photons. *Optica* **4**, 1006–1010 (2017).

[115] Renner, R., Gisin, N. & Kraus, B. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A* **72**, 012332 (2005).

[116] Renner, R. & Cirac, J. I. de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography. *Phys. Rev. Lett.* **102**, 110504 (2009).

[117] Renner, R. & König, R. Universally Composable Privacy Amplification Against Quantum Adversaries. In *Proceedings of the Second Theory of Cryptography Conference (TCC) 2005*, vol. 3378 of *Lecture Notes in Computer Science*, 407–425 (Springer, Berlin, 2005).

[118] van Assche, G. *Quantum cryptography and secret-key distillation* (Cambridge University Press, Cambridge, 2006).

[119] Tanzilli, S. *et al.* Highly efficient photon-pair source using periodically poled lithium niobate waveguide. *Electron. Lett.* **37**, 26–28 (2001).

[120] Waks Edo *et al.* Secure communication: Quantum cryptography with a photon turnstile. *Nature (London)* **420**, 762–762 (2002).

[121] Alléaume, R. *et al.* Experimental open-air quantum key distribution with a single-photon source. *New J. Phys.* **6**, 92 (2004).

[122] Intallura, P. M. *et al.* Quantum key distribution using a triggered quantum dot source emitting near 1.3μm. *Appl. Phys. Lett.* **91**, 161103 (2007).

[123] Heindel, T. *et al.* Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range. *New J. Phys.* **14**, 083001 (2012).

[124] Rau, M. *et al.* Free space quantum key distribution over 500 meters using electrically driven quantum dot single-photon sources—a proof of principle experiment. *New J. Phys.* **16**, 043003 (2014).

[125] Takemoto, K. *et al.* Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors. *Sci. Rep.* **5**, 14383 (2015).

[126] Leifgen, M. *et al.* Evaluation of nitrogen- and silicon-vacancy defect centres as single photon sources in quantum key distribution. *New J. Phys.* **16**, 023021 (2014).

[127] Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on Practical Quantum Cryptography. *Phys. Rev. Lett.* **85**, 1330–1333 (2000).

[128] Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **61**, 052304 (2000).

[129] Hwang, W.-Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.* **91**, 057901 (2003).

[130] Wang, X.-B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).

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

[132] Ma, C. *et al.* Silicon photonic transmitter for polarization-encoded quantum key distribution. *Optica* **3**, 1274–1278 (2016).

[133] Sibson, P. *et al.* Integrated silicon photonics for high-speed quantum key distribution. *Optica* **4**, 172–177 (2017).

[134] Wang, S. *et al.* 2 GHz clock quantum key distribution over 260 km of standard telecom fiber. *Opt. Lett.* **37**, 1008–1010 (2012).

[135] Bell, J. S. On the Problem of Hidden Variables in Quantum Mechanics. *Rev. Mod. Phys.* **38**, 447–452 (1966).

[136] Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed Experiment to Test Local Hidden-Variable Theories. *Phys. Rev. Lett.* **23**, 880–884 (1969).

[137] Giustina, M. *et al.* Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons. *Phys. Rev. Lett.* **115**, 250401 (2015).

[138] Shalm, L. K. *et al.* Strong Loophole-Free Test of Local Realism. *Phys. Rev. Lett.* **115**, 250402 (2015).

[139] Barrett, J., Hardy, L. & Kent, A. No Signaling and Quantum Key Distribution. *Phys. Rev. Lett.* **95**, 010503 (2005).

[140] Acín, A. *et al.* Device-Independent Security of Quantum Cryptography against Collective Attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).

[141] Acín, A., Massar, S. & Pironio, S. Efficient quantum key distribution secure against no-signalling eavesdroppers. *New J. Phys.* **8**, 126 (2006).

[142] Pironio, S. *et al.* Device-independent quantum key distribution secure against collective attacks. *New J. Phys.* **11**, 045021 (2009).

[143] Vazirani, U. & Vidick, T. Fully Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **113**, 140501 (2014).

[144] Briegel, H.-J., Dür, W., Cirac, J. I. & Zoller, P. Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication. *Phys. Rev. Lett.* **81**, 5932–5935 (1998).

[145] Wootters W. K. & Zurek W. H. A single quantum cannot be cloned. *Nature (London)* **299**, 802–803 (1982).

[146] Deutsch, D. *et al.* Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels. *Phys. Rev. Lett.* **77**, 2818–2821 (1996).

[147] Lo, H.-K. & Chau, H. F. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science* **283**, 2050–2056 (1999).

[148] Shor, P. W. & Preskill, J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000).

[149] Kraus, B., Gisin, N. & Renner, R. Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication. *Phys. Rev. Lett.* **95**, 080501 (2005).

[150] Tomamichel, M., Lim, C. C. W., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **32**, 634 (2012).

[151] Grosshans, F. & Cerf, N. J. Continuous-Variable Quantum Cryptography is Secure against Non-Gaussian Attacks. *Phys. Rev. Lett.* **92**, 047905 (2004).

[152] Navascués, M., Grosshans, F. & Acín, A. Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography. *Phys. Rev. Lett.* **97**, 190502 (2006).

[153] García-Patrón, R. & Cerf, N. J. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Phys. Rev. Lett.* **97**, 190503 (2006).

[154] Furrer, F. *et al.* Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks. *Phys. Rev. Lett.* **109**, 100502 (2012).

[155] Leverrier, A. Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States. *Phys. Rev. Lett.* **114**, 070501 (2015).

[156] Scarani, V. QKD: a million signal task. In Horodecki, R., Kilin, S. Y. & Kowalik, J. (eds.) *Quantum Cryptography and Computing*, 76–82 (IOS Press, 2010).

[157] Scarani, V. & Renner, R. Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing. *Phys. Rev. Lett.* **100**, 200501 (2008).

[158] Leverrier, A., Grosshans, F. & Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **81**, 062343 (2010).

[159] Sheridan, L. & Scarani, V. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A* **82**, 030301 (2010).

[160] Law, C. K. & Eberly, J. H. Analysis and Interpretation of High Transverse Entanglement in Optical Parametric Down Conversion. *Phys. Rev. Lett.* **92**, 127903 (2004).

[161] Franson, J. D. Nonlocal cancellation of dispersion. *Phys. Rev. A* **45**, 3126–3132 (1992).

[162] Lodewyck, J. *et al.* Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **76**, 042305 (2007).

[163] Weedbrook, C. *et al.* Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621–669 (2012).

[164] Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A: Math. Phys. Engineer. Sci.* **461**, 207–235 (2005).

[165] Cai, R. Y. Q. & Scarani, V. Finite-key analysis for practical implementations of quantum key distribution. *New J. Phys.* **11**, 045024 (2009).

[166] Sheridan, L., Le, T. P. & Scarani, V. Finite-key security against coherent attacks in quantum key distribution. *New J. Phys.* **12**, 123019 (2010).

[167] Sheridan, L. & Scarani, V. Erratum: Security proof for quantum key distribution using qudit systems [Phys. Rev. A 82, 030301(R) (2010)]. *Phys. Rev. A* **83**, 039901(E) (2011).

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

[169] Lo, H.-K., Chau, H. F. & Ardehali, M. Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security. *Journal of Cryptology* **18**, 133–165 (2005).

[170] Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photon.* **7**, 378–381 (2013).

[171] Robinson, B. S. *et al.* 781 Mbit/s photon-counting optical communications using a superconducting nanowire detector. *Opt. Lett.* **31**, 444–446 (2006).

[172] Stucki, D. *et al.* High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.* **11**, 075003 (2009).

[173] Fröhlich, B. *et al.* Long-distance quantum key distribution secure against coherent attacks. *Optica* **4**, 163–167 (2017).

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

[175] Bunandar, D., Zhang, Z., Shapiro, J. H. & Englund, D. R. Practical high-dimensional quantum key distribution with decoy states. *Phys. Rev. A* **91**, 022336 (2015).

[176] Bao, H., Bao, W., Wang, Y., Zhou, C. & Chen, R. Finite-key analysis of a practical decoy-state high-dimensional quantum key distribution. *J. Phys. A: Mathematical and Theoretical* **49**, 205301 (2016).

[177] Ribordy, G., Brendel, J., Gautier, J.-D., Gisin, N. & Zbinden, H. Long-distance entanglement-based quantum key distribution. *Phys. Rev. A* **63**, 012309 (2000).

[178] Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks. *Phys. Rev. Lett.* **111**, 130501 (2013).

[179] Costa, B., Mazzoni, D., Puleo, M. & Vezzoni, E. Phase Shift Technique for the Measurement of Chromatic Dispersion in Optical Fibers Using LED's. *IEEE Transactions on Microwave Theory and Techniques* **30**, 1497–1503 (1982).

[180] Derickson, D. (ed.) *Fiber Optic Test and Measurement.* Hewlett-Packard professional books (Prentice Hall PTR, 2007).

[181] Rosenberg, D., Kerman, A. J., Molnar, R. J. & Dauler, E. A. High-speed and high-efficiency superconducting nanowire single photon detector array. *Opt. Express* **21**, 1440–1447 (2013).

[182] Kerman, A. J. *et al.* Kinetic-inductance-limited reset time of superconducting nanowire photon counters. *Appl. Phys. Lett.* **88**, 111116 (2006).

[183] Kerman, A. J., Rosenberg, D., Molnar, R. J. & Dauler, E. A. Readout of superconducting nanowire single-photon detectors at high count rates. *Journal of Applied Physics* **113**, 144511 (2013).

[184] Dauler, E. A. *et al.* Review of superconducting nanowire single-photon detector system design options and demonstrated performance. *Opt. Eng.* **53**, 081907 (2014).

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

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

[187] Yoshino, K.-I. *et al.* High-speed wavelength-division multiplexing quantum key distribution system. *Opt. Lett.* **37**, 223–225 (2012).

[188] Grein, M. E., Stevens, M. L., Hardy, N. D. & Dixon, P. B. Stabilization of Long, Deployed Optical Fiber Links for Quantum Networks. In *Conference on Lasers and Electro-Optics*, FTu4F.6 (Optical Society of America, 2017).

[189] Wiseman, H. M., Jones, S. J. & Doherty, A. C. Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox. *Phys. Rev. Lett.* **98**, 140402 (2007).

[190] Jones, S. J., Wiseman, H. M. & Doherty, A. C. Entanglement, Einstein-Podolsky-Rosen correlations, Bell nonlocality, and steering. *Phys. Rev. A* **76**, 052116 (2007).

[191] Skrzypczyk, P., Navascués, M. & Cavalcanti, D. Quantifying Einstein-Podolsky-Rosen Steering. *Phys. Rev. Lett.* **112**, 180404 (2014).

[192] Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419–478 (2014).

[193] Saunders D. J., Jones S. J., Wiseman H. M. & Pryde G. J. Experimental EPR-steering using Bell-local states. *Nat. Phys.* **6**, 845–849 (2010).

[194] Smith Devin H. *et al.* Conclusive quantum steering with superconducting transition-edge sensors. *Nat. Commun.* **3**, 625 (2012). 10.1038/ncomms1628.

[195] Bennet, A. J. *et al.* Arbitrarily Loss-Tolerant Einstein-Podolsky-Rosen Steering Allowing a Demonstration over 1 km of Optical Fiber with No Detection Loophole. *Phys. Rev. X* **2**, 031003 (2012).

[196] Wittmann, B. *et al.* Loophole-free Einstein–Podolsky–Rosen experiment via quantum steering. *New J. Phys.* **14**, 053030 (2012).

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

[198] Branciard, C., Cavalcanti, E. G., Walborn, S. P., Scarani, V. & Wiseman, H. M. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Phys. Rev. A* **85**, 010301 (2012).

[199] Bao, H.-Z. *et al.* Time–energy high-dimensional one-side device-independent quantum key distribution. *Chinese Physics B* **26**, 050302 (2017).

[200] Schneeloch, J., Dixon, P. B., Howland, G. A., Broadbent, C. J. & Howell, J. C. Violation of Continuous-Variable Einstein-Podolsky-Rosen Steering with Discrete Measurements. *Phys. Rev. Lett.* **110**, 130407 (2013).

[201] Dixon, P. B., Howland, G. A., Schneeloch, J. & Howell, J. C. Quantum Mutual Information Capacity for High-Dimensional Entangled States. *Phys. Rev. Lett.* **108**, 143603 (2012).