Progress Toward Quantum Communications Networks: Opportunities and Challenges

Article *in* Proceedings of SPIE - The International Society for Optical Engineering · March 2007

DOI: 10.1117/12.708669

CITATIONS
9

READS
227

16 authors, including:

Thomas Chapuran
Perspecta Labs
65 PUBLICATIONS **879** CITATIONS
SEE PROFILE

Paul Toliver
Vencore Labs
119 PUBLICATIONS **1,413** CITATIONS
SEE PROFILE

Nicholas Peters
Oak Ridge National Laboratory
80 PUBLICATIONS **1,459** CITATIONS
SEE PROFILE

Richard J. Hughes
Los Alamos National Laboratory
200 PUBLICATIONS **3,821** CITATIONS
SEE PROFILE

Progress Toward Quantum Communications Networks: Opportunities and Challenges

Robert J. Runser[*a,b], Thomas Chapuran[a], Paul Toliver[a], Nicholas A. Peters[a], Matthew S. Goodman[a], Jon T. Kosloski[b], Nnake Nweke[b], Scott R. McNown[b], Richard J. Hughes[c], Danna Rosenberg[c], Charles G. Peterson[c], Kevin P. McCabe[c], Jane E. Nordholt[c], Kush Tyagi[c], Philip A. Hiskett[c], Nicholas Dallmann[c]

[a]Telcordia Technologies, 331 Newman Springs Rd., Red Bank, NJ 07701

[b]Laboratory for Telecommunications Sciences, 8080 Greenmead Drive, College Park, MD 20740

[c]Los Alamos National Laboratory, Los Alamos, NM 87545

ABSTRACT

Quantum communications is fast becoming an important component of many applications in quantum information science. Sharing quantum information over a distance among geographically separated nodes using photonic qubits requires a reconfigurable transparent networking infrastructure that can support quantum information services. Using quantum key distribution (QKD) as an example of a quantum communications service, we investigate the ability of fiber networks to support both conventional optical traffic and single-photon quantum communications signals on a shared infrastructure. The effect of Raman scattering from conventional channels on the quantum bit error rate (QBER) of a QKD system is analyzed. Additionally, the potential impact and mitigation strategies of other transmission impairments such as four-wave mixing, cross-phase modulation, and noise from mid-span optical amplifiers are discussed. We also review recent trends toward the development of automated and integrated QKD systems which are important steps toward reliable and manufacturable quantum communications systems.

Keywords: quantum key distribution, quantum communications, optical networking, QKD, single-photon detection, Raman scattering, optoelectronic integration

1. INTRODUCTION

Transmitting quantum information between two geographically separated parties is becoming a critical technology for the realization of many of the promises of quantum information science. The first practical application of quantum information science, quantum key distribution (QKD), has already stimulated the commercialization of quantum security systems and devices. QKD systems use photonic qubits (quantum bits) to transfer quantum information through free-space and fiber optic links for the establishment of a perfectly secure cryptographic key between two parties. The engineering progress that has been made in the development of QKD systems in research and commercial laboratories has paved the way for many other emerging applications of quantum communications.

This paper discusses the opportunities enabled by quantum communications and the challenges presented in deploying quantum communications on existing networks. The advantages provided by quantum communications in cryptography and other quantum information applications are discussed in this section. The critical elements for enabling photonic quantum communications networks are introduced in Section 2 and progress in long distance transmission is reviewed. Section 3 presents an analysis of co-existence transmission where quantum and conventional optical signals share the same fiber optic link. The recent development of automated QKD systems and prospects for integrated "QKD systems-on-a-chip" are also discussed in Section 4, followed by our conclusions in Section 5.

1.1 Quantum Key Distribution (QKD)

The ever increasing reliance on electronic information systems for the storage, processing, and transfer of valuable data has made security one of the most important aspects in system design. Most data is secured by encrypting it with algorithms based on computational-complexity that require the distribution of cryptographic keys using symmetric or

*rrunser@ieee.org; phone (240) 373-5085

public key techniques. The security of these algorithms relies on the assumption that the minimum time it would take to decipher the encrypted message without access to the key is known given state-of-the-art technology. The security assurance provided by computationally complex algorithms is that the information will no longer be relevant by the time an adversary could complete the operations required to decipher the encrypted message.

Although it may be possible to make predictions based on technological trends such as Moore's Law, history has also taught us that it is difficult to anticipate ground-breaking innovations in technology or mathematics that might call these security assumptions into question. For example, Ron Rivest, one of the inventors of the RSA public key distribution algorithm, published a security challenge in 1977: factor a 129-bit number to decode a secret message. At the time, Rivest was certain that the factoring problem would take millions of years even on the most powerful computers expected to be available in the future. Amazingly, the number was factored in 1994 by a group of researchers led by Bellcore (now Telcordia), MIT, Iowa State University, and Oxford University[1]. Advances in factoring techniques enabled the group to decipher the secret message long before the original predictions would have otherwise indicated. Other breakthrough advances in computation are also possible in the future which could challenge today's security assumptions. For example, the realization of a quantum computer of sufficient scale to exercise the efficient quantum factoring algorithm proposed by Peter Shor[2] would have a disruptive impact on the security of the Public Key Infrastructure (PKI) used in most secure communications today.

A different method of encryption, which is not susceptible to advances in mathematics or computing, is the Vernam-Mauborgne one-time pad invented in 1917. Each binary bit of the message is XORed with a bit from the key or pad which is as long as the message. In 1949, Claude Shannon formally proved that a perfectly random one-time pad was impervious to known ciphertext attacks[3]. While elegant in principle, the one-time pad has several implementation challenges. The key must be as long as the message and securely delivered to the communicating parties (using a trusted courier for instance). This is a rather daunting task when one considers the vast amount of data that is encrypted every day and that each of the keys would have to be physically transported over great distances. The logistics of key distribution in one-time-pad cryptography have dramatically limited its usefulness.

A new approach to the key distribution problem, however, may offer a potential solution and eventual realization of unconditional security. Unlike cryptography based on computational complexity, the security principles of quantum key distribution are rooted in the laws of quantum physics. QKD has the potential to continuously distribute secure keys over communications networks, including free-space and fiber optic links, without compromising the security of the key or relying on unproven computational and mathematical assumptions. The security in QKD is achieved by encoding random data in the quantum states of individual photons, transmitting the photons over a quantum channel, and performing a protocol, BB84 for example, to distill a final, shared secret key[4]. One of the important security principles of BB84 is the detection of eavesdropping. In BB84, the transmitter chooses between two "conjugate" bases for encoding her qubits. The non-orthogonality of these quantum states makes it impossible for an eavesdropper to measure the qubit values with perfect fidelity. When an eavesdropper makes a measurement on a qubit that is in a superposition of states, the quantum system is reduced to only one of the two possible states by the eavesdropper's detector. This perturbation to the original state can be used to detect the presence of an eavesdropper on a quantum channel who is attempting to actively measure and re-transmit the quantum bit sequence. The actions of the eavesdropper on the channel will introduce errors and make her presence known to the communicating parties through an increase in the quantum channel bit error rate. Indeed, steps of the QKD protocol allow the communicating parties, typically referred to as Alice and Bob, to detect and defeat eavesdropping on their communications by an adversary often referred to as Eve.

QKD has several unique security advantages:

- *Quantum bits used in the key cannot be recorded by Eve.* Photons that Eve passively extracts and measures are not received by Bob and do not become part of the key. Eve's attempt to actively measure and retransmit bits to Bob will increase Bob's error rate and expose her tampering attempts.
- *More powerful computing technologies do not help Eve guess the key.* QKD does not use mathematical complexity to protect the information exchanged between Alice and Bob. As a result, more powerful computing techniques, including quantum computing, do not help Eve obtain the key.
- *Alice and Bob can exchange a secure key in Eve's presence.* Post-processing steps such as privacy amplification in QKD protocols attribute errors in the quantum channel to Eve's tampering. Alice and Bob use information theoretic estimates to determine the size of their final key to ensure its security. In BB84, a secure key can be established for quantum bit error rates (QBER) approximately less than 11%[5].

- *Security is based on the known laws of physics.* The security of QKD rests on the fundamental assumptions of quantum mechanics including superposition and the no-cloning theorem. For Eve to mount a successful and undetectable attack on an ideal QKD system, she must demonstrate that these assumptions can be violated.

The widespread adoption of QKD systems will ultimately be motivated by analysis of the threats to the current network security infrastructure, comparisons with traditional cryptographic approaches, and realization of scalable and practical multi-user quantum networks. Nonetheless, QKD is a valuable technique that can be used to achieve unconditionally secure key distribution.

1.2 Quantum Communications for Other Applications

Although QKD is the first practical application of quantum information science, many new concepts are beginning to emerge that can leverage the photonic quantum communications technologies that QKD has stimulated. For example, quantum communications will be required to efficiently network quantum computers and to facilitate distributed quantum computing over distances ranging from a few meters for photonic qubit interconnects to hundreds of kilometers for geographically separated computing nodes. Photonic qubits transported by fiber optic interconnects and cables can serve as a quantum channel for these applications. Quantum communications techniques can also be used to distribute entanglement over a distance. The geographic distribution of quantum mechanically entangled states can improve clock synchronization where knowledge of precise locations is not required[6]. Finally, other security applications for quantum communications, such as entanglement-based voting, have been proposed to improve the security and privacy of elections[7]. For these applications and others yet to be discovered, quantum communications networks will be critical for enabling the sharing and exchange of quantum information.

2. QUANTUM COMMUNICATIONS NETWORKS

Since the early QKD demonstrations of the 1990s, many research groups throughout the world have begun experimental investigations to show the applicability of quantum communications over distances that are of practical interest for securing networks. Both weak coherent and entangled qubits have been shown to propagate into the hundred kilometer range for free-space and dedicated-fiber optic links. In 2002, the Los Alamos group achieved terrestrial free-space QKD through a 10-km air mass at ground level in daylight, demonstrating the feasibility of QKD from a ground station to a low earth orbiting satellite[8]. Today the longest distance free-space link that has been demonstrated to distribute keys was over 144 km at night using an entanglement-based QKD scheme[9]. Fiber QKD has also made a tremendous amount of progress. In 2003 a group from Mitsubishi[10] reported a fiber distance over 87 km. This was quickly exceeded in 2004 by a Toshiba group[11] which achieved 122 km. To date, the world record in fiber QKD is held by Los Alamos which demonstrated a distance of 185 km working in collaboration with the superconducting Transition Edge Sensor (TES) detector group at NIST-Boulder and Albion College[12].

Practical constraints in QKD system deployment, such as optical loss in the transmission medium and precision tolerances of the components, appear to limit the current generation of QKD systems to about 200 km. Breakthroughs in on-demand single-photon sources[13,14], noiseless single-photon detectors[15,16], and novel optical fiber types[17] could improve the reach of these systems in the future. It may also be possible to take advantage of new protocols to extend the transmission distance such as the decoy state protocol[18]. By using a combination of these innovations, QKD systems may be able to move beyond metropolitan area fiber distances in the near future.

Although point-to-point quantum communications are important, multi-user quantum networking will require that Alice can route her quantum communications to other parties. Many of the approaches used in conventional optical networks can also route quantum channels. Optical micro electro-mechanical systems (MEMS), for instance, can establish an optical route for quantum communications between nodes connected to a transparent optical network[19]. If Alice's QKD transmitter uses a tunable laser, wavelength routing architectures, such as those employed in wavelength division multiplexed (WDM) passive optical networks (PONs), are also a possibility. Most low-loss optical switching devices are compatible with quantum networks provided that the optical path is nearly free from in-band noise and does not require the quantum channel to traverse an amplifying medium.

The majority of demonstrated QKD systems have focused on free-space line-of-sight paths or dedicated "dark" optical fiber links for supporting the quantum channel between Alice and Bob. Such point-to-point links, however, are not scalable or cost effective for QKD to achieve widespread deployment especially in multi-user quantum networks. Access to dedicated dark-fiber can be costly, especially if it is needed to all destinations of interest for the quantum service. Furthermore, Alice and Bob still require a conventional network connection to exchange classical information

to complete the QKD protocol and a means to transmit their encrypted information. For these reasons, it is important to investigate the compatibility of quantum communications with conventional optical channels on the same fiber infrastructure, and the technical challenges associated with upgrading an existing optical network to support quantum communications services.

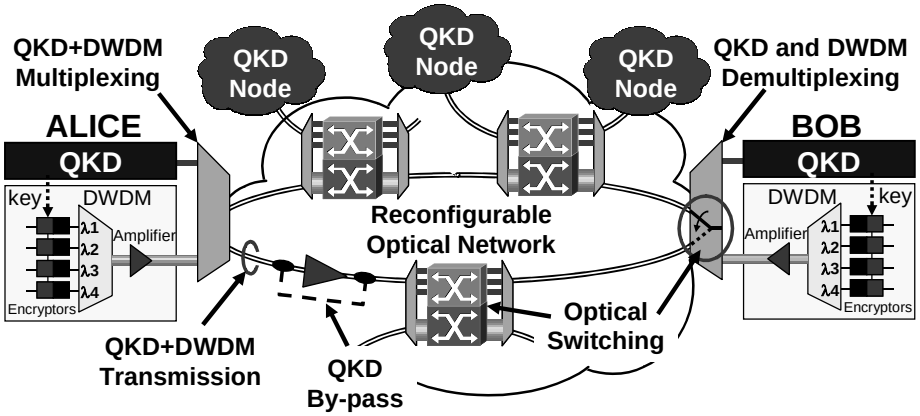


Fig. 1. Transparent multi-user optical network supporting QKD and DWDM channels on the same infrastructure.

Figure 1 shows a vision of a future multi-user network that supports both quantum and conventional optical communications. One or more quantum wavelengths may be assigned to single-photon transmitters allocated to the quantum band. Conventional channels, such as those from Dense Wave Division Multiplexing (DWDM) systems, are also present on the network. The network has several design features that are required to maintain adequate isolation between the quantum and conventional optical signals including:

- *QKD and DWDM multiplexing.* Spontaneous emission noise from optical amplifiers and conventional optical signals at the transmitting nodes is eliminated from the quantum channel band.
- *QKD and DWDM co-existence transmission.* The optical channel plan minimizes the transmission impairments that impact the quantum channels. These impairments include noise generated by conventional channels and nonlinear interactions with the quantum signals that impact the fidelity of the photonic qubits.
- *QKD bypass.* The noise from amplified spontaneous emission (ASE) intrinsic to optical amplification can severely impact the error rate of the quantum channel. The spectral components of the ASE noise that are in-band with the quantum signal reduce the fidelity of the received qubits[20]. The network should enable quantum signals to bypass elements that are not compatible with quantum channels such as optical amplifiers and opaque nodes that convert the optical signal into the electronic domain.
- *Optical switching.* Switching elements that route quantum communications or implement optical network protection should not introduce cross-talk from conventional channels into the quantum band. The switch architecture should also minimize optical loss for the quantum signals.
- *QKD demultiplexing*. High-isolation demultiplexing of the conventional and quantum channels at the receiver is a critical component of the co-existence architecture. Typical isolations should exceed 100 dB. Quantum channel band-pass filtering may also be needed to eliminate other sources of noise.

A practical guideline for ensuring that the co-existence network does not constrain the performance of the quantum communications system is to limit the in-band contribution to the noise to a level less than the quantum system detector dark noise. However, advanced single-photon detector technologies are being developed which have almost no intrinsic background dark counts[15]. For these systems, the detectors themselves may be a useful metrology tool for characterizing the network noise levels. Despite these challenges, recent work suggests that the co-existence of quantum and conventional channels on the same network is possible. The technical constraints of co-existence networks and the impact of noise background levels are described in the next section.

3. CO-EXISTENCE OF QUANTUM AND CONVENTIONAL COMMUNICATIONS

Overlaying quantum communications services onto existing fiber networks leverages the installed infrastructure and enables lower cost deployment of quantum services. There are several challenges, however, in implementing this architecture. The single-photon nature of the quantum communications signal makes them extremely sensitivity to noise on the fiber network. In this section, experiments that characterize the fiber environment at the levels required for single-photon transmission are discussed, and their impact on QKD systems is analyzed.

3.1 Multiplexing and Demultiplexing Quantum and Conventional Communications Channels

In order to multiplex quantum and conventional signals onto the same fiber infrastructure, the noise properties of the conventional system must be well characterized to avoid introducing noise into the quantum band. A practical bound for this noise in the quantum band can be set by the single-photon receiver dark count limit. Most fiber QKD systems use InGaAsP avalanche photodiodes (APDs) in Geiger mode. These detectors can have dark count probabilities ranging from 1E-04 to 1E-07 per 1-ns gate time. In terms of optical average power, noise in the quantum band should be approximately less than -138 dBm or 16 attowatts (which corresponds to 1.24E-07 photons per nanosecond in the 1550-nm band) to not adversely impact the performance of a QKD system with a dark count probability of 1E-07. Noise at such low levels is not considered in conventional network design. For the network to meet this condition, it may be necessary to characterize the noise using single-photon detectors themselves as a measurement tool.

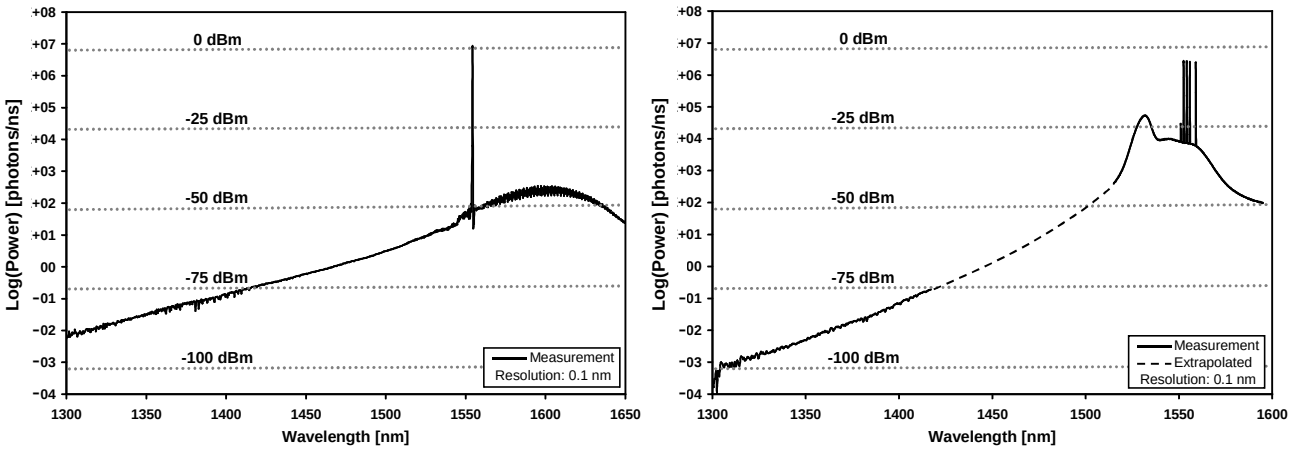


Fig. 2. Wide optical spectra of (a) DFB laser at 0 dBm and (b) EDFA amplifying 4 wavelengths each to -5 dBm. The dynamic range was extended for wavelengths < 1500 nm by suppressing the peaks and combining the resulting spectra.

Spontaneous emission noise from distributed feedback (DFB) communications lasers and Erbium-doped optical amplifiers (EDFAs) are two examples of conventional optical noise sources that could impair the quantum band. Figure 2 shows a high dynamic range, wideband optical spectra from two types of devices operating at normal levels for conventional DWDM networks. For the purposes of comparing the noise levels to quantum receiver dark count probabilities, it is convenient to express the average power in terms of photons/ns. (On this scale, a typical 0-dBm conventional channel at 1550 nm has a photon rate of approximately 8E+ 06 photons/ns.) For conventional applications, the DFB laser exhibits an excellent signal-to-noise ratio (approx. 50 dB). However, the spontaneous emission in the 1550-nm region is in the hundreds of photons/ns—well above the threshold to support quantum communications using single photons. Both components exhibit observable noise characteristics well into the 1300-nm band where the noise level is approximately 1E-02 to 1E-03 photons/ns. For quantum communications in the low noise 1300-nm region, low cost, wideband high-isolation 1300/1550-nm thin-film filters[21] can be used to limit the spontaneous background in the 1300-nm region to an acceptable level. For quantum communications in the same band as the conventional channels, multi-channel, high-isolation optical multiplexers could be used to control the extent of broadband emission into adjacent channels. Alternatively, a deep notch filter based on a fiber Bragg grating for instance, could be used to "carve out" a low-noise region of the spectrum to support a quantum channel. In this case, the adjacent channel suppression or depth of the notch must be greater than 60 dB to limit spontaneous noise from the DFB laser or more than 75 dB in the case of the EDFA. Since each active optical component will have different spectral properties, the noise must be well characterized and understood to prevent unwanted leakage into the quantum band.

The quantum channel filter requirements at the receiver are more stringent than at the transmitter. The quantum band filter must nearly eliminate all cross-talk from conventional optical sources at the demultiplexer. In addition, the quantum signal, which has traversed some distance through optical fiber and other components, may be reduced to a level very near the dark noise limit of the single-photon detector. Given a typical WDM channel power of -15 dBm at a conventional receiver, a quantum band demultiplexer must have a channel isolation of more than 120 dB. Additional bandpass filtering may also be required to reduce the impact of scattered light on the quantum system as discussed in the next subsection.

3.2 Scattering Noise

The generation of optical noise in the quantum band from the propagation and interaction of conventional channels with the fiber is one of the most important design considerations for the channel plan and filtering requirements of a co-existence network. Once noise enters the quantum channel passband, it cannot be removed by additional filtering and will inevitably increase the quantum bit error rate of the receiver. Scattering of light from conventional optical signals as they propagate in fiber is the most serious source of in-band quantum channel noise. Conventional optical signals act as "pumps" for three dominant scattering processes: Rayleigh, Brillouin, and Raman. The spectra of Brillouin and Rayleigh scattering are confined to the region very near the pump wavelength. Rayleigh is an elastic scattering process where the energy and spectral bandwidth of the scattered photons are nearly identical to the bandwidth of the pump. Rayleigh scattering is more often observed in the counter-propagating direction. Brillouin scattering is an inelastic process where pump photons are scattered off acoustic phonons in the fiber yielding lower energy scattered photons predominantly in the opposite direction of the pump. The spectral bandwidth of the photons produced by spontaneous Brillouin scattering is about 10 to 20 GHz. Both Rayleigh and Brillouin scattering can add significant noise power to the quantum signal when the quantum channel is allocated very near (<< 100 GHz) a conventional channel. However, meeting the necessary adjacent channel isolation requirements at the receiver when the quantum signal is that close to a conventional channel is a much more difficult constraint and limits the minimum channel spacing to at least 100 GHz.

Rayleigh and Brillouin backscattered light from conventional signals, however, can impact the performance and operation of bi-directional QKD systems. The "plug-and-play" architecture[22], which is the most common example of a bi-directional QKD system, uses a conventional optical pulse emitted by Bob toward Alice to initiate the QKD session. Alice modulates and attenuates the pulse to the single-photon level and reflects it back to Bob on the same fiber using a Faraday mirror. This bi-directional architecture automatically compensates for polarization variations along the fiber path. In these bi-directional systems, the quantum receiver may detect backscattered light from the initial conventional pulse that is sent by Bob. Unfortunately wavelength filtering cannot be used here since the conventional pulse is equivalent in spectrum to the expected single-photon signal modulated and returned by Alice. Instead, time-multiplexing or "burst mode" operation is used to avoid gating Bob's detectors while the conventional pulses are being transmitted. The communications rate of bi-directional systems is ultimately limited by the backscatter characteristics of the conventional pulses.

Raman scattering of conventional optical signals is a much more severe limitation to the performance of quantum communications systems in co-existence networks, and can have important consequences on the network channel plan. Raman scattering is an inelastic mechanism where light interacts with vibrational modes (optical phonons) in the fiber. At room temperature, light can scatter from a conventional optical channel to both higher and lower energy bands far from the original optical pump frequency. The Raman scattering spectrum is divided into Stokes and anti-Stokes bands. In Stokes scattering, a higher energy pump photon scatters into a lower energy photon and optical phonon. This mechanism has been extensively studied as a means for optical amplification when stimulated scattering is encouraged by a lower energy signal near the peak of the Stokes emission spectra. Anti-Stokes scattering occurs when an optical photon from the pump combines with an existing optical phonon in the fiber to produce a higher energy photon. Although much weaker than the Stokes process, noise levels comparable in strength to the quantum communications channel can be generated by spontaneous anti-Stokes scattering.

The general Raman pump and signal interaction can be described by two coupled differential equations,

$$\frac{dP}{dz} = -\alpha_1 P + \beta_1 S + \gamma_1 PS \tag{1}$$

$$\frac{dS}{dz} = -\alpha_2 S + \beta_2 P + \gamma_2 PS\,, \tag{2}$$

where P and S are the pump and signal powers, respectively, and α, β, and γ are the wavelength-dependent fiber attenuation, spontaneous Raman scattering coefficient, and stimulated Raman scattering coefficient, respectively. For spontaneous scattering into the quantum band which is supporting very low signal powers, the stimulated scattering terms ($\gamma_1 PS$ and $\gamma_2 PS$) and the spontaneous scattering from signal to pump ($\beta_1 S$) can be neglected. The signal power, which represents the scattered noise, can then be solved in closed form[23] as a function of the propagation distance, z.

Previously, we have experimentally investigated the co-existence of quantum signals in the 1300-nm band with conventional DWDM channels in the 1550-nm band. For a system with a dark count level near 1E-03 photons/ns, we demonstrated impairment free multiplexing of a QKD channel and commercial optical DWDM system supporting 4 wavelength channels with an aggregate power of + 2 dBm over 25 km of SMF-28® fiber[24]. We have also shown that at least 170-nm separation between a 1310-nm QKD signal and + 6-dBm conventional channel near the 1550-nm band was required in order to maintain an adequate quantum bit error rate for this system and its filter architecture[25]. In both cases, anti-Stokes Raman scattering was the dominant noise source after the conventional channels were rejected from the quantum receiver by filtering. We have found that simple filtering architectures and wide channel spacings can be used to ensure that the scattered light does not impair the quantum channel. Additionally the filters used for isolating the 1300-nm quantum band and 1550-nm conventional band are low cost[21] and can be cascaded to produce band separations of more than 120 dB.

Recently, there has been interest in investigating the co-existence of 1550-nm quantum channels with conventional signals[26] since this is the lowest loss region of optical fiber and where the longest distance quantum communications experiments have been achieved. In addition to the filter and isolation challenges imposed by multiplexing and separating the quantum channel from signals in the conventional band, Raman scattering can ultimately limit the performance of these systems under certain constraints.

In order to analyze the impact of Raman scattering on a QKD system operating in the 1550-nm band, we use a model for predicting the QBER performance of the system in the presence of in-band noise contributed by Raman scattering. The system QBER can be expressed[27] as the ratio of the total error rate, R_{Error} , to the rate of total QKD detection events which is the sum of the total error rate and sifted bit rate, R_{Sifted}:

$$QBER = \frac{R_{Error}}{R_{Error} + R_{Sifted}} \quad . \tag{3}$$

For a BB84 system, the sifted bit rate can be calculated as

$$R_{Sifted} = \tfrac{1}{2} q \, \mu \, T(z) T_{Rx} \eta \, f_{rep} \, , \tag{4}$$

where q accounts for losses associated with the interferometer architecture when photon energy falls outside of the central interference peak, μ is the average single-photon number per pulse transmitted by Alice, $T(z)$ is the transmissivity of the link as a function of distance, T_{Rx} is the transmissivity of Bob's interferometer, η is Bob's detector efficiency, and f_{rep} is Bob's detector gating rate. The leading factor of 1/2 accounts for the 50% protocol efficiency of BB84.

The error rate has three main contributors: detector dark noise (R_{Det}), imperfect interference (R_{Opt}), and background noise (R_{Noise}). The sum of these three contributions gives the total rate of errors:

$$R_{Error} = R_{Det} + R_{Opt} + R_{Noise} \tag{5}$$

The dark count contribution to the error rate is given by

$$R_{Det} = \tfrac{1}{4} \, p_d \, n f_{rep} \, , \tag{6}$$

where p_d is the dark count probability per gate and n is the number of detectors in Bob's apparatus. Since 50% of the dark counts occur when Alice and Bob do not choose the same basis, they do not contribute to the error rate. Of the remaining 50% that occur when they choose the same basis, half will contribute to the correct bit value. The factor of 1/4 accounts for the 25% of the time when dark counts cause errors. For simplicity, we have neglected the contribution of detector afterpulsing to the detector error rate. The effect of afterpulsing is negligible if the detectors are gated at a sufficiently low rate to allow enough time for the traps in the detectors to empty. The errors associated with afterpulsing can also be minimized by implementing afterpulse blocking circuitry in the system[28].

Imperfect interference in Bob's interferometer can cause errors when photons detected in the correct basis are received by the wrong detector. The contribution to the error rate that is associated with Bob's interferometer, R_{Opt}, can be related to the interferometer visibility, V, as:

$$R_{Opt} = R_{Sift}(1-V) \tag{7}$$

Finally, the noise contribution to the error rate can be expressed as

$$R_{Noise} = \tfrac{1}{4}\, p_n \eta\, n f_{rep} \tag{8}$$

and depends upon the probability of a noise photon falling within the detection gating interval, p_n, the detector quantum efficiency, and the number of detectors in Bob's system. Similar to the dark count probability, noise photons will only contribute to the error rate 25% of the time. In the case of the co-existence network, the probability of a noise event falling within Bob's detector gating interval can be a function of several other parameters associated with the QKD link. When Raman scattering from conventional channels on the same fiber contributes to noise at the QKD wavelength, p_n is a function of the launch power of the conventional channels, the frequency separation of the conventional and quantum channels, and the propagation distance. The noise probability is determined by calculating the average noise power for a given co-existence scenario (distance, conventional channel power, channel spacing, etc.) and expressing p_n in terms of photons/gate.

Table. 1. QKD System Parameters using in Model

Detector dark count probability (p_d)	1.0E-06	counts/gate
Detector gate width	1	ns
Detector quantum efficiency (η)	20	%
Transmitted avg. photon number (μ)	0.1	photons/pulse
Transmitted photon pulse width	<<1	ns
Visibility (V)	99	%
Bob optical losses ($\propto 1/T_{Rx}$) (includes filter losses)	5	dB
q	0.5	(phase modulation)
Number of detectors (n)	2	(BB84)
QKD wavelength (variable)	1500-1600	nm
QKD bandpass filter width	0.01	nm
QKD bandpass filter shape	Rectangular	(ideal)

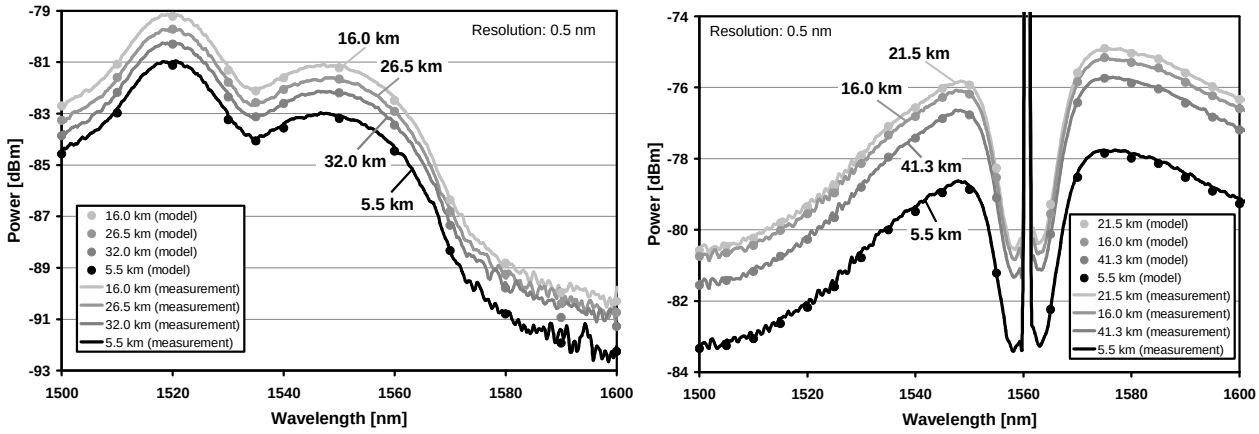
We use the total system QBER as the figure of merit for comparing the performance of a QKD system operating in the 1500 to 1600-nm range in a co-existence network to the same system operating over dark-fiber. Since all detection rates are a function of f_{rep}, the term can be eliminated from the QBER ratio so that the QBER is independent of the system repetition rate. Information theoretic proofs require that the QBER be less than 11% to yield secret bits that can be used to generate cryptographic keys[5]. The parameters used in this model are summarized in Table 1 and approximate the best reported results from an APD-based, phase-modulated QKD system[29].

To understand the limitations imposed on a 1550-nm band QKD system in the co-existence regime, we measured the spontaneous Raman response of SMF-28e® over several fiber lengths for two cases: 1) Stokes noise in the 1550-nm band from a conventional CW channel at 1310 nm and 2) Stokes and anti-Stokes noise from a conventional channel in the 1550-nm band. The parameters for the two cases are summarized in Table 2. Figure 3 shows sample spectra of the spontaneous Raman noise for several lengths of fiber in each case. From this experimental data, we estimated the spontaneous Raman coupling term, β_2, from (2) to generalize the Raman response for these two regimes.

Table. 2. Conventional Wavelength Channel Parameters

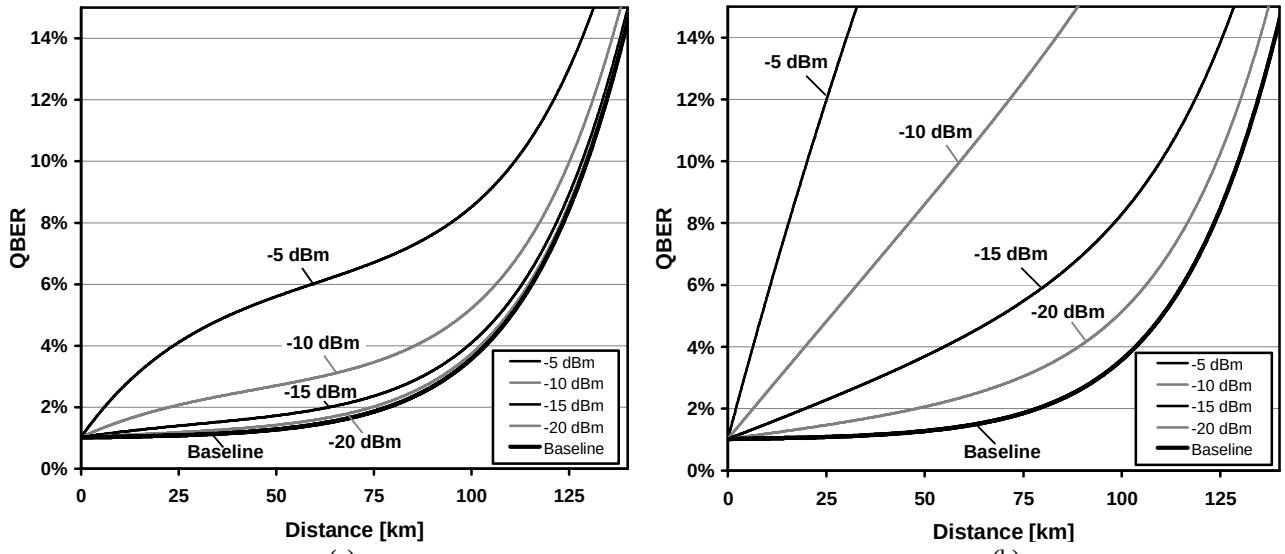
Parameter	Case 1	Case 2	
CW wavelength	1310	1560	nm
CW fiber loss	0.330	0.185	dB/km
CW launch power	variable	variable	

Using the wavelength-dependent fiber losses from our measurements, we compared the QBER performance of a QKD system with a variable wavelength in the 1500 to 1600-nm region. The conventional channel is assumed to be fully extinguished by the QKD band demultiplexer and passband filters and the only contributions to the in-band optical noise are from Raman scattering.



(a) (b)

Fig. 3. Measured fiber Raman scattering spectra for various fiber distances and points from the model: (a) Case 1: 1310-nm CW channel with 2.98-dBm launch power and (b) Case 2: 1560-nm CW channel with 0.84-dBm launch power.



(a) (b)

Fig. 4. QBER for (a) Case 1: 1310-nm CW and 1530-nm QKD channels and (b) Case 2: 1560-nm CW and 1530-nm QKD channels. The CW power is varied as a parameter from -5 to -20 dBm. The Baseline is the dark noise limit (no CW).

The QBER response as a function of propagation distance is shown in Figure 4(a) and (b) for Case 1 and Case 2 respectively, both with the QKD wavelength fixed at 1530 nm. The average launch power at the transmitter of the 1310 and 1560-nm CW channels are varied between -5 and -20 dBm for each of the two cases. For comparison, the baseline

QBER of a system operating on a dark-fiber link is also shown. In Case 1, the QKD channel experiences the Stokes Raman scattering from a 1310-nm conventional channel that is nearly 33 THz away from the quantum signal. In Case 2, the QKD signal experiences anti-Stokes Raman scattering from a nearby 1560-nm conventional channel that is about 4 THz from the QKD signal. The QKD system operating in the anti-Stokes regime experiences a much stronger effect from the nearby 1560-nm convention channel than the QKD system in the Stokes regime where the conventional signal is much further away. At a 1310-nm CW launch power of -20 dBm, the QBER response in Case 1 nearly overlaps the performance of the dark-fiber system where the dominant contribution to the QBER is the detector dark noise. However, the system in Case 2 experiences an increase in QBER from the nearby conventional signal even at CW launch powers as low as -20 dBm, which is well below the launch power of most optical communications systems.

This model can also be used to determine the optimal QKD wavelength in the 1500 to 1600-nm regime for the two cases studied. Fixing the CW channel power to -15 dBm, the QBER for various QKD wavelengths is plotted as a function of distance in Figure 5. The QBER for the system operating on the same fiber as the conventional 1310-nm CW channel in Case 1 outperforms the system operating in the same band as the 1560-nm conventional channel in Case 2. As shown in Figure 5(a), the QKD system in Case 1 performs better the further away it is from the conventional signal. The best QKD operating wavelengths are in the region > 1570 nm. The small peak in the Raman Stokes spectrum near 1520 nm makes this wavelength the noisiest of the channels in the 1500 to 1600-nm region. Although it may appear that better performance may be achieved by increasing the wavelength beyond 1600 nm, fiber losses will also increase due to the infrared absorption in standard, singlemode fibers and ultimately limit the system performance.

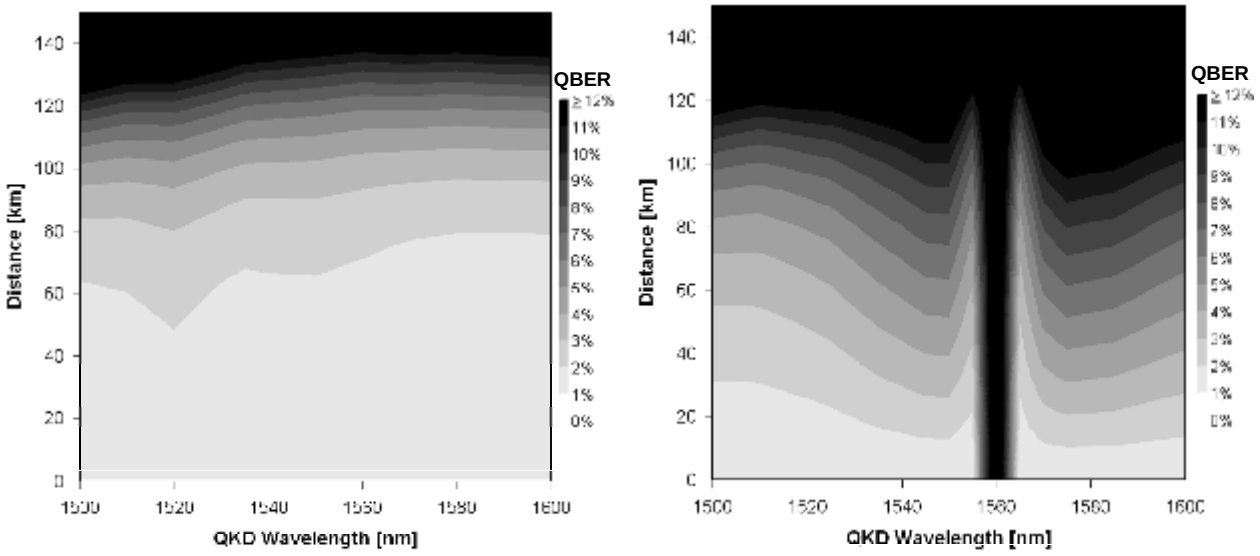


Fig. 5. QBER as a function of the QKD wavelength and propagation distance when the conventional channel launch power is fixed at -15 dBm for (a) Case 1 and (b) Case 2. QBER contours are represented by the grayscale level indicated on the vertical legend. QBER increases with darker shading.

For Case 2, the QKD system experiences a noticeable increase in QBER for distances > 50 km across the 1500 to 1600-nm band. The region directly overlapping with the CW channel at 1560 nm is forbidden but the low noise dips near the carrier between 1555 and 1565 nm, as previously seen in Fig. 3(b), provide a marginal improvement relative to the worst performing wavelengths at 1550 and 1575 nm. However, operating near the 1560-nm carrier increases the isolation requirements on the QKD bandpass filter and may limit the practicality of operating in this narrow low noise region.

From these results, network operators that want to support quantum communications services must take the impact of Raman scattering into account when assigning channels to the quantum band. In general, the lowest noise operating point for most co-existence networks will be the anti-Stokes regime where the QKD channel is at a shorter wavelength than the conventional signals. The optimum quantum channel allocation minimizes the QBER by striking the right balance between minimum optical attenuation and minimum in-band noise for a given transmission distance. It is usually advantageous to operate as far away from the conventional channels as possible in order to relax the constraints on the filter isolation and passband bandwidth requirements at the quantum receiver.

Other parameters can also be varied in QKD systems to improve the co-existence performance in the 1550-nm region. Although the filter bandwidth (0.01 nm) in this analysis is near the transform limit of typical 200-ps QKD signal pulses, it is possible to narrow the detector gate time below 1 ns to reduce the impact of the noise. It is also possible, although not always desirable, to operate the conventional channels at lower powers or support quantum services in co-existence networks for shorter distance (<< 100 km) applications where Raman scattering levels do not play a significant role. Recently, QKD co-existence with DWDM channels in the same spectral region around 1550 nm was demonstrated[26] over 50 km. In this experiment, a narrow bandpass filter (~ 1 GHz) isolated the quantum signal from the conventional channels and noise background. Impairment free operation of the system near the dark noise limit was realized when the conventional signals were launched at a peak power of approximately -20 dBm. For conventional power levels greater than -20 dBm, the system QBER was observed to increase.

3.3 Four-wave Mixing Impairment

Another important transmission effect to consider in co-existence networks are nonlinear effects that can give rise to unacceptable noise levels in the quantum channel band. Four-wave mixing (FWM) among the conventional channels is one effect that can have implications on the allocation of quantum wavelengths. Since the refractive index of glass changes with optical intensity and the total intensity is proportional to the sum of the individual DWDM channel electric fields *squared*, new product terms are generated during fiber transmission and appear as additional components in the optical spectrum. Given three co-propagating signals at frequencies f_i, f_j, and f_k, a new signal is generated at frequency f_{ijk}, where,

$$f_{ijk} = f_i + f_j - f_k \qquad i, j \neq k \tag{9}$$

Modern DWDM systems are designed with channels on an ITU-designated frequency grid, spaced at 50, 100, or 200 GHz. As a result, the new product terms that are generated as a result of FWM will fall on the same frequency grid. Some of these terms overlap with the original DWDM channels, causing inter-channel interference, and DWDM systems are currently designed to keep the penalty due to this interference to a minimum. However, a number of FWM products will be generated outside the spectrum of the occupied DWDM channels. While these out-of-band terms can generally be safely ignored in a conventional DWDM system, their impact can be critical when determining the optimal quantum channel wavelength in a co-existence network. If the resulting FWM component spectrum overlaps with the QKD channel passband, the signal-to-noise ratio will be reduced, leading to an increased QBER.

The efficiency of the FWM process and the noise that results is dependent upon a number of link parameters including DWDM channel power, fiber dispersion, difference frequency of DWDM spectral components, fiber nonlinear coefficient, and polarization alignment. In order to manage the impact of FWM on a given co-existence link, certain parameters can be optimized. For example, since the magnitude of the FWM components fall off as one moves further away in frequency, it is possible to position the QKD channel relatively far away from the DWDM channels. This can be accomplished, for example, by placing the QKD channel at 1310 nm while leaving the DWDM channels in the 1550-nm band. A second approach is to reduce the individual DWDM channel powers. Since the FWM component has a cubic dependence on channel power (assuming equal power levels on channels *i, j, k*), the FWM noise power drops off relatively quickly with decreasing channel power. However, one disadvantage to this approach is a potential reduction in the ultimate transmission length for the DWDM channels due to power and noise budget issues. A final approach is to optimize the fiber dispersion map with spans of predominantly high local dispersion, so that phase matching between DWDM channels can be minimized. We are currently in the process of evaluating FWM effects and determining necessary system requirements for robust co-existence of QKD and DWDM channels, both through the use of simulations and experiments.

3.4 Cross-phase Modulation

Although an extremely low noise environment is crucial for the operation of a co-existence network, nonlinear interactions between the quantum and conventional signals can also affect the fidelity of the qubits and the system QBER. The same nonlinear characteristics of the optical fiber that introduce noise through four-wave mixing also decrease the fidelity of differential phase-encoded qubits through cross-phase modulation (XPM). XPM is a mechanism by which a relatively intense optical signal alters the phase of another signal that co-propagates with it on the same fiber. As a relatively strong conventional signal propagates with a weak single-photon quantum communications channel, the effective index of refraction experienced by the quantum signal becomes a function of the conventional channel intensity and interaction length in the fiber. Since most fiber-based QKD systems use differentially-encoded phase to transmit

quantum information[27], the relative phase between the two pulses (or peaks) of the quantum wave function carrying the phase information must also be preserved during fiber propagation. XPM can increase the system QBER if the phase of one of the two pulses is altered significantly with respect to the other. The increase in QBER due to the degradation in the fidelity of a phase-encoded qubit can be calculated as a reduction of the interferometer visibility, *V*.

The XPM interaction between the quantum and conventional signals depends on the conventional signal power and the length over which the signals interact on the fiber. This length is referred to as the effective length, L_{eff}, and represents the total distance that the two pulses of the quantum signal propagate with conventional signals of *different* intensity. Fortunately, L_{eff} is not necessarily the distance between Alice and Bob and can be limited by the wavelength dependence of the fiber refractive index. Since the index of refraction experienced by the conventional and quantum signals will be different, they will travel past each other after some distance in the fiber. The effective length is the distance over which one of the pulses of the quantum wave function propagates with a conventional signal that the other pulse does not and vice versa. It can be shown that L_{eff} in this interaction scenario is given by

$$L_{eff} = \min\left\{ \frac{n(\lambda_c)\delta_A - c\tau}{\left| n(\lambda_q) - n(\lambda_c) \right|}, \quad L_{link} \right\} \tag{10}$$

where c is the speed of light in vacuum, $n(\lambda_q)$ and $n(\lambda_c)$ are the frequency dependent indices of refraction experienced by the quantum and conventional signals respectively, τ is the temporal width of the conventional signal, δ_A is the path length difference in the arms of Alice's unbalanced interferometer, and L_{link} is the total fiber distance between Alice and Bob.

When the conventional and quantum signals are in different bands, as in Case 1 analyzed in Section 3.2, L_{eff} can be rather small compared to the length of the link between Alice and Bob, and the effect of XPM will be minimal. However, when the signals are in the same band, as in Case 2, L_{eff} will be on the same order of magnitude as L_{link}. The magnitude of the XPM effect depends on several properties of the conventional channels including their intensity, pulse width, data modulation rate and format, data pattern statistics, and polarization alignment and wavelength difference with respect to the quantum signal. As a result of these factors, the impact of XPM on the QBER is statistical. A detailed analysis of this interaction is currently underway. Preliminary results indicate that XPM is unlikely to be the dominant impairment in co-existence networks with conventional channels transporting random data on wavelengths with typical power levels and modulation formats used in today's optical networks.

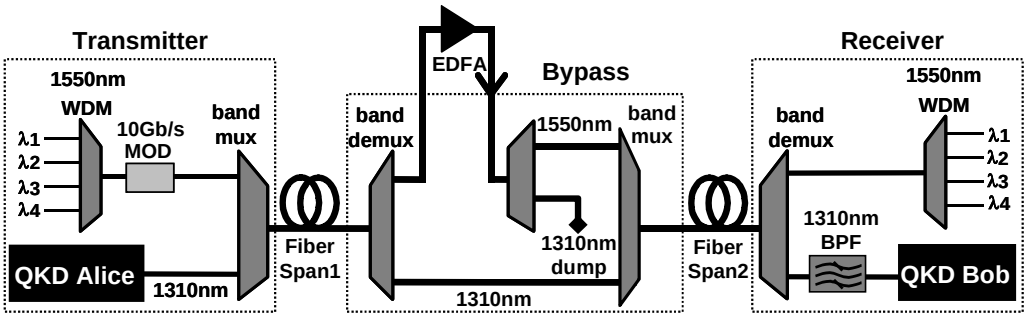


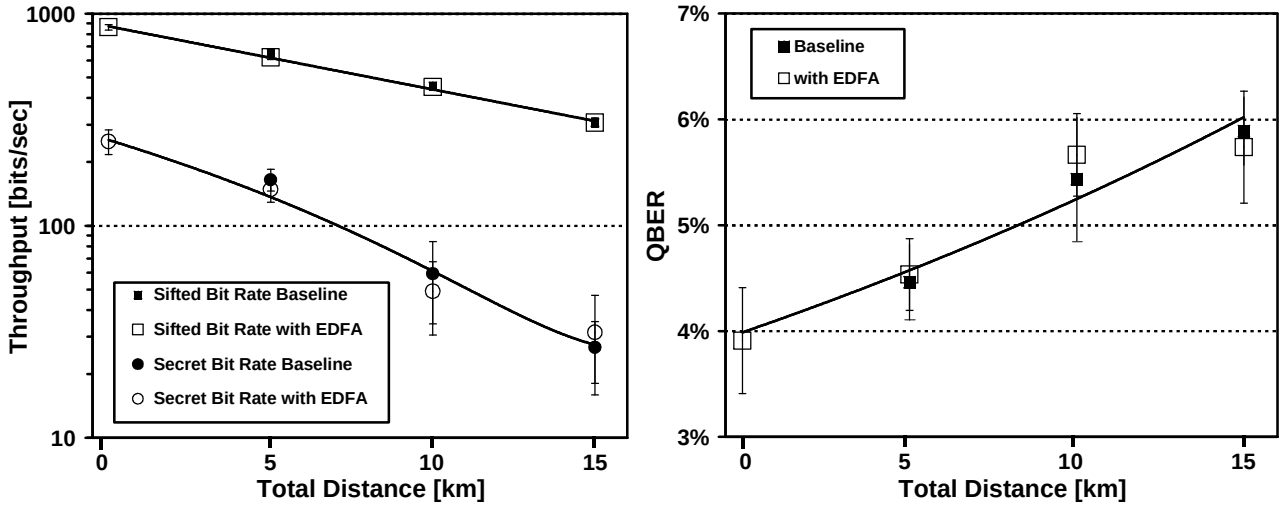
Fig. 6. Quantum channel bypass architecture for co-existence with in-line EDFAs.

3.5 Quantum Communications Channel Bypass

Most fiber networks today rely on inline amplification of the conventional signals to span distances greater than 50 km. Band-limiting the noise from amplifiers at the transmitter and receiver nodes has previously been discussed in Section 3.1. However, it is also important to be able to transmit quantum signals over WDM links containing inline optical amplifiers between fiber spans. An optical amplifier bypass that enables quantum signals to avoid passing through optical amplifiers is shown in Figure 6. In this example, the 1310-nm band supports the quantum service and the 1550-nm band is used for conventional WDM transport. Similar to previous demonstrations of QKD and WDM co-existence, broadband noise from the conventional channels is eliminated at the terminal nodes by high-isolation band multiplexer/demultiplexer filters. An additional bandpass filter centered on the 1310-nm quantum channel at the

receiver reduces the impact of Raman scattering noise after fiber propagation. The EDFA is located mid-span between the two terminals. The bypass is designed with a similar band mux/demux arrangement in order to separate the quantum channel from the WDM signals at the amplifier node. The 1550-nm band WDM signals are routed to the EDFA for amplification while the 1310-nm quantum signal traverses a separate, low-loss dark-fiber path. Two band filter stages are used following the output of the EDFA to eliminate the 1310-nm spontaneous noise from the amplified WDM signal. When the WDM and quantum signals are re-combined at the output of the bypass, the potential sources of in-band noise on the quantum channel have been sufficiently reduced.

To demonstrate the operation of the amplifier bypass, a quantum signal at 0.5 photons/pulse was generated by a 100-kHz phase-based B92 QKD system[30] and multiplexed with four 10-Gb/s WDM channels centered at 1550 nm onto the same transmission fiber. An EDFA was located at a mid-span node along the fiber transmission link. The noise rejection in the 1310-nm QKD band of the amplified WDM signals was > 120 dB. In addition, isolation of the 1550-nm band was > 30 dB at the 1310-nm port of the first band demultiplexer at the bypass input to avoid WDM interference effects that could occur when the two fiber paths are recombined again at the bypass output. In the absence of the EDFA, the insertion losses of the bypass filters through the 1550 and 1310-nm paths were 1.9 and 1.3 dB respectively. The peak power of each WDM channel was set to -25 dBm at the input to the bypass to emulate a realistic mid-span amplification scenario. The net gain, including the insertion loss of the filters, for each of the four WDM channels was 20 dB.



(a) (b)

Fig. 7. QKD system performance through the EDFA bypass node: (a) QKD throughput and (b) QBER vs. fiber distance.

The QKD system sifted and secret key rates, and quantum bit error rate were experimentally measured over a variety of fiber distances, where the total fiber distance is the sum of the individual span lengths on either side of the amplifier bypass. The baseline QKD system performance without the amplifier inserted into the bypass was compared to the case with the amplifier and WDM channels present. As shown in Figure 7, the presence of the EDFA and amplified WDM channels did not significantly impair the QKD system performance compared to the system baseline. The primary impairment to the QKD system was loss though the fiber and filters as evidenced by the linear behavior of the initial sifted bits on the log scale of Figure 7. The reduction in the secret bit rate at 15 km is a result of an increased QBER and subsequent compression of the final key by the privacy amplification algorithm as the system approaches the dark noise limit of the single-photon detectors.

An amplifier bypass architecture for enabling the co-existence of 1310-nm quantum communications with conventional WDM channels has been demonstrated. This filter architecture is also capable of bypassing other active or opaque nodes which are not compatible with quantum communications signals. This architecture is relatively easy to implement and an inexpensive upgrade to existing networks for quantum channels in the 1300-nm band. A similar approach could be used for quantum signals multiplexed with WDM channels both in the 1550-nm band. However, the filtering and noise suppression requirements are more challenging to achieve when the quantum and conventional channels are in closer proximity to each other.

4. AUTOMATED AND INTEGRATED QKD SYSTEMS

The recent commercialization of QKD systems has dramatically reduced their operating complexity as compared to earlier laboratory demonstration systems. Automated QKD operation is a necessary step to enable the widespread use of QKD without requiring specialized training or knowledge of quantum physics. A fully automated system should adapt to changing network conditions that are typical on fiber networks such as variation in the state of polarization and changes in propagation delay and loss associated with network path reconfiguration.

We have constructed and demonstrated a fully automated one-way phase-based BB84 system that is compatible with reconfigurable fiber optic networks[28]. The system consists of two workstation-sized computer cases that house all of the electronics and optics needed to perform QKD. The system uses an Ethernet connection separate from the quantum channel for the public communications involved in the QKD protocol. We have demonstrated the system operating over distances of up to 75 km at a mean photon number of 0.4 photons/pulse. The system incorporates features that enhance the compatibility with dynamic, reconfigurable optical networks such as afterpulse-blocking detector circuitry and automated, real-time polarization optimization. (Although the system uses phase modulation, the phase modulators are polarization sensitive and require active polarization alignment.) This system also includes a novel auto-synchronization technique to temporally align the gated single-photon detectors with the incoming quantum signal using only the detected events from the quantum channel. By incorporating Rubidium clocks in the transmitter and receiver, an accurate sub-nanosecond time reference can be obtained by sweeping the single-photon detector gates periodically through a specified time interval to generate a photon arrival rate histogram at the receiver. This information is used to dynamically center the detector gates on the information bearing quantum interference peak. Since this "quantum clock recovery" process is operating periodically, the QKD system can track slow (a few seconds) frequency and phase drifts in the single-photon arrivals to keep the single-photon gates aligned without requiring external synchronization channels. The auto-synchronization algorithm can also re-acquire the quantum signal after network reconfiguration events within a few minutes. We have recently demonstrated fully-automated QKD signal acquisition after path reconfiguration using a MEMs switch inserted into the path of the quantum signal[31]. The system has operated over a 25-km in-ground dark-fiber on the ATDNet network in the Washington, D.C. area[32] over an extended period with an average transmitted photon number of 0.2 photons/pulse and generated tens of millions of authenticated, privacy amplified secret key bits.

Full integration of the optical and electronic components for QKD systems is the next important step for reducing the complexity and improving the manufacturability and performance of QKD systems. As QKD systems move from small scale research prototypes to more widely deployed systems, issues of manufacturability and reproducibility of component performance characteristics and reliability become important. The ability to manufacture quality components in quantity, however, drives lower cost manufacturing, which concomitantly lowers the overall systems cost. The greatest cost reduction available in optoelectronic technologies stems from optoelectronic integration, which reduces component test and packaging costs – which often dominate the manufacturing costs.

For QKD, integration may provide significant performance, stability, and reliability advantages. There are several areas where such integration can prove particularly important. In the case of the Mach Zehnder interferometers in phase-based QKD systems, integration can miniaturize these devices significantly using well-known techniques[33]. The impact of integration on the interferometer temperature stability alone (due to smaller component size) is likely worth the effort in addition to the significant improvements expected in phase drift and polarization stability. It is also possible to use integration techniques to obtain polarization independence between the interferometer arms[34]. Similarly, integration of the single-photon sources and phase modulators along with associated control and monitoring electronics (such as drivers and advanced diagnostics) enable greater functionality at the transmitter with lower cost. Integrated single-photon detectors and their associated electronics in a III-V material system has a similar impact on the QKD receiver. Both applications could use monolithic or multi-chip hybrid approaches to form the primary elements of "QKD systems-on-a-chip."

Finally, optoelectronic integration can enable the use of novel technologies that could change the QKD landscape. While weak coherent QKD systems are the most widely studied currently, it is desirable to move toward QKD systems that utilize inherently single-photon sources, including quantum dots[14] and other exotic sources such as diamond lattices[13] which depend on device integration techniques.

5. CONCLUSIONS

Over the last 10 years, tremendous progress has been made to extend the reach of fiber QKD systems and to show their compatibility with DWDM optical networks in order to provide secure communications. QKD is an important first step toward the distribution and sharing of quantum information over geographic distances using photonic qubits. Although challenges remain in defining a low-noise quantum communications channel plan, the technology for implementing QKD services on metropolitan area fiber networks exists today. By carefully analyzing the noise generated by conventional optical channels at the single-photon level and understanding the interaction mechanisms between quantum and conventional signals as they co-propagate, networks can be upgraded to support quantum communications services. Automated QKD systems have been developed that operate on conventional in-ground reconfigurable networks without requiring operator knowledge of the underlying physics or engineering principles of quantum communications systems. Integration of the components in a QKD system onto a single chip is the next critical step toward realizing manufacturable, compact, and low-cost systems. Integrated quantum devices are an important driver for the development of quantum communications services and the networks that will support those services in the future.

ACKNOWLEDGEMENT

We are grateful for support of this work from the Disruptive Technology Office and the Laboratory for Telecommunications Sciences.

REFERENCES

1. D. Atkins, M. Graff, A.K. Lenstra, P.C. Leyland, *Asiacrypt*, pp. 263-277, 1994.
2. P.W. Shor, *Proc. 35th Annual Symposium on Foundations of Computer Science*, pp. 124-134, 1994.
3. C.E. Shannon, *Bell System Technical Journal*, vol. 28, pp. 656-715 (1949).
4. C.H. Bennett, G. Brassard, *Proc. Intl. Conf. Comp. Sys. & Sig. Proc.*, Bangalore, India, pp. 175–179, Dec. 1984.
5. N. Lütkenhaus, *Phys. Rev. A*, vol. 59, 3301 (1999).
6. R. Jozsa, D.S. Abrams, J.P. Dowling, C.P. Williams, *Phys. Rev. Lett.*, vol. 85, pp. 2010-2013 (2000).
7. M. Hillery, M. Ziman, V. Buzek, M. Bielikova, *Phys. Lett. A*, vol. 349, p. 75 (2006).
8. R.J. Hughes, J.E. Nordholt, D. Derkacs, C.G. Peterson, *New Journal of Physics*, vol. 4, pp. 43.1-43.14 (2002).
9. R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, et al., *arXiv:quant-ph/0607182*, v 2, Jul 2006.
10. T. Hasegawa, T. Nishioka, H. Ishizuka, J. Abe, M. Matsui, S. Takeuchi, *CLEO/QELS*, Baltimore, MD, 2003.
11. C. Gobby, Z.L. Yuan, A.J. Shields, *Appl. Phys. Lett.*, vol. 84, pp. 3762-3764 (2004).
12. P.A. Hiskett, D. Rosenburg, C. G Peterson, R.J. Hughes, S. Nam, et al., *New Journal of Physics*, vol. 8, 193 (2006).
13. J.R. Rabeau, F. Jelezko, A. Stacey, B.C. Gibson, et al., *LEOS Summer Topical Meetings*, p. 15, July 17-19, 2006.
14. J. Vuckovic, D. Fattal, C. Santori, G.S. Solomon, Y. Yamamoto, *arXiv:quant-ph/0307025*, v 1, 3 Jul 2003.
15. D. Rosenberg, S. Nam, P.A. Hiskett, C.G. Peterson, R.J. Hughes, et al., *Appl. Phys. Lett.*, vol. 88 021108 (2006).
16. B.S. Robinson, A.J. Kerman, E.A. Dauler, R.J. Barron, D.O. Caplan, et al., *Opt. Lett.*, vol. 31, pp. 444-446 (2006).
17. G. Humbert, J. Knight, G. Bouwmans, P. Russell, et al., *Optics Express*, vol. 12, pp. 1477-1484 (2004).
18. W.-Y. Hwang, *Phys. Rev. Lett*. vol. 91, p. 057901 (2003).
19. P. Toliver, R.J. Runser, T.E. Chapuran, J.L. Jackel, et al., *IEEE Photon. Technol. Lett.*, vol. 15, p. 1669 (2003).
20. S. Fasel, N. Gisin, G. Ribordy, V. Scarani, H. Zbinden, *Phys. Rev. Lett.*, vol. 89, 107901 (2002).
21. See for example: http://www.valdor.com/products00/bpf5.html
22. H. Zbinden, J.-D. Gautier, N. Gisin, B. Huttner, A. Muller, W. Tittel, *Electron. Lett.*, vol. 33, pp. 586-588 (1997).
23. T. E. Chapuran, P. Toliver, R. J. Runser, S. R. McNown, et al., *Proc. of SPIE*, vol. 5815, pp. 164-175, May, 2005.
24. R.J. Runser, T.E. Chapuran, P. Toliver, M.S. Goodman, J. Jackel, et al., *OFC '05*, Anaheim, CA, March 6-11, 2005.
25. N.I. Nweke, P. Toliver, R. J. Runser, S. R. McNown, et al., *Appl. Phys. Lett.*, vol. 87, 174103 (2005).
26. T.J. Xia, D.Z. Chen, G. Wellbrock, A. Zavriyev, A.C. Beal, K.M. Lee, *OFC '06*, Anaheim, CA, March 6-10, 2006.
27. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, *Rev. Mod. Phys.*, vol. 74, pp. 145–195 (2002).
28. R.J. Hughes, T.E. Chapuran, N. Dallmann, P.A. Hiskett, et al., *Proc. SPIE*, vol. 5893, 589301 (Aug. 24, 2005).
29. C. Gobby, Z.L. Yuan, A.J. Shields, *Appl. Phys. Lett.*, vol. 84, pp. 3762-3764 (2004).
30. R. J. Hughes, G. L. Morgan, C. G. Peterson., *J. Mod. Optics*, vol. 47, pp. 533-547 (2000).
31. R.J. Runser, T.E. Chapuran, P. Toliver, M.S. Goodman, et al., *OFC '06*, Anaheim, CA, March 6-10, 2006.
32. R.J. Runser, P. Toliver, S. McNown, *LEOS 2002*, Glasgow, Scotland, Nov. 10-14, 2002.
33. B.E. Little, *OFC '03*, Atlanta, GA, March 23-28, 2003.
34. Y. Nambu, K. Yoshino, A. Tomita, *Jpn. J. Appl. Phys.*, vol. 45, pp. 5344 (2006).