Key Pre Distribution Using Quantum Key Channel – A Survey

MD.Sarwar Pasha[1], A. Bala Ram[2]

[1]M.Tech. Student, CSE Dept., CMR Institute of Technology, Hyderabad, A.P
Email-id: pashamohd42@gmail.com
[2]Associate Professor, CSE Dept., CMR Institute of Technology, Hyderabad, A.P
Email-id: balaram.balaram@gmail.com

Abstract

Modern optical networking techniques have the potential to greatly extend the applicability of quantum communications by moving beyond simple point-to-point optical links, and by leveraging existing fibre infrastructures. We experimentally demonstrate many of the fundamental capabilities that are required. These include optical-layer multiplexing, switching, and routing of quantum signals; quantum key distribution (QKD) in a dynamically reconfigured optical network; and coexistence of quantum signals with strong conventional telecom traffic on the same fibre. We successfully operate QKD at 1310 nm over a fibre shared with four optically amplified data channels near 1550 nm. We identify the dominant impairment as spontaneous anti- Stokes Raman scattering of the strong signals, quantify its impact, and measure and model its propagation through fibre. We describe a quantum networking architecture which can provide the flexibility and scalability likely to be critical for supporting widespread deployment of quantum applications.

Index Terms- Quantum key distribution, multiple access, cryptography

1. Introduction

The ultimate usefulness of most communications services depends strongly on the ability to network, i.e., to efficiently connect many end users with each other or with shared resources. Much of the experimental research on Quantum Key Distribution (QKD) has focused on improving transmission performance over a fixed end-to-end connection between a single pair of quantum endpoints, Alice and Bob. However, this type of connectivity does not scale well, because the level of resources that are required increases very rapidly with the number of end users. Efficient networking solutions are clearly needed to move QKD and other types of quantum communications beyond the realm of niche deployments.

Many of the technologies, components and techniques needed to address these problems have been developed over the past quarter century for use in conventional optical fibre networks.

Early fibre networks utilized optics solely for point-to-point (PTP) transmission between opaque nodes, in which all networking functions were implemented electronically. In contrast, modern fibre networks increasingly take advantage of optical transparency, in which a subset of critical networking functions such as switching, routing and multiplexing are preferentially performed in the optical layer [1]. This enables the establishment of multiple optically transparent lightpaths through a network domain, and highly dynamic re-routing or reconfiguration of these lightpaths.

Applied to QKD, optical networking offers the prospect of flexible and scalable on- demand connectivity for a large number of Alice-Bob pairs. End-to-end key establishment over an untrusted network is feasible for lightpaths compatible with the maximum attenuation allowed

Current address: DARPA/DSO, 3701 North Fairfax Dr., Arlington VA 22203; work performed while affiliated with Telcordia by the QKD system. Communications over longer end-to-end paths, or between endpoints with incompatible QKD systems, can be routed on demand via a shared set of 'trusted relay' nodes in secured locations [2-8]. The network can also provide endpoints with optically transparent access to other shared resources, such as 'centralized' entangled-photon sources for QKD. Finally, optical networking offers the prospect of leveraging costly infrastructure already deployed for telecom and enterprise networks, via wavelength-division multiplexing (WDM) of quantum and conventional data signals onto the same fibres. A central question for the future of QKD is to what extent it can attain wide applicability by taking advantage of these major advances in conventional optical networking.

Achieving this vision requires developing new capabilities, and validating them in realistic network environments. In this paper, we experimentally demonstrate a number of fundamental capabilities of optical networking as applied to QKD. These include optical routing, automated restoration after network path reconfiguration, and multiplexing and transmission of QKD with strong conventional WDM channels on the same fibre. We also examine practical considerations for applying optical networking architectures and technologies to QKD, and resulting impacts on the quantum signals in these environments. Although the experiments and analyses reported in this paper focus entirely on QKD, many of the results are likely to also carry implications for a broader range of quantum communications services which rely on the transport of photonic qubits over fibre networks.

The earliest QKD optical networking experiments were reported by Townsend's group [9-10], which measured quantum bit error rates (QBER) for QKD signals transmitted through a 1:3 passive optical splitter to facilitate distribution of QKD signals to three different receivers. Following this work, several additional groups proposed passive fibre distribution networks to transmit key to multiple nodes [11-13]. Our group reported the first demonstrations of QKD through optical switches, including key establishment through several types of switch fabrics, and optical protection switching between two fibre paths connecting Alice and Bob [14]. Honjo et al. used a planar lightwave circuit (PLC) switch to connect Alice with either of two Bobs, demonstrating low QBER in the presence of crosstalk from a much stronger channel on a different path through the switch [15]. Optical switching has also been used in a portion of the DARPA quantum network [8], and investigated in a three-node QKD configuration at NIST [16].

The first experiment using WDM to combine QKD with an uncorrelated data channel on the same fibre was reported by Townsend [17]. WDM is often employed for carrying 'bright' synchronization pulses along with the quantum signals, and has occasionally been used to support one or a small number of data channels. However, few experiments have reflected the environments encountered in routing quantum signals through a modern telecom or enterprise network, in which very strong (~1 mW) data channels create substantial impairments which must be understood and mitigated. Early work with multi-channel WDM can be found in [18, 19] and [20], for QKD signals near 1310 nm or 1550 nm, respectively.

Our approach differs from, but is complementary with, the ‘trusted relay’ backbone architecture demonstrated by the SECOQC collaboration [2-4], and related approaches [5] which build on concepts developed for the DARPA quantum network [6-8]. For example, the SECOQC network is constructed from a collection of fixed PTP QKD links, with a variety of QKD technologies, connecting opaque quantum nodes in secured locations. Networking functions are performed entirely in the electronic domain, in a trusted network dedicated to QKD.

The following section provides a brief overview of the role of optical networking in quantum communications. Section 3 presents experimental results on the operation of QKD in dynamically reconfigurable networks, while Section 4 reports results on combining QKD with strong data channels in shared network environments. Section 5 provides a summary and conclusions.

2. Our Contribution

Well-known techniques in classical multiple access optical communications were applied to quantum cryptography applications. That enabled multiple users to exchange secret keys, via an optical network, without trusting any other nodes. The proposed setups offered key features that would facilitate their deployment in practice. In all of them, classical communications services were integrated with that of quantum on a shared platform, which would substantially reduce thecost for public and private users. More generally, by sharing network resources among many users, the total cost per user would shrink, making the deployment of such systems more feasible. Another cost-saving feature in our setups was their relying on only one QKD detection module per user. The setups considered were inspired by existing optical access networks as well as future all-optical networks.

3. Literature Survey

Among all the methods of encryption ever devised, only one has been proven to be information-theoretically secure, i.e. secure against an eavesdropper who has unbounded ability. It is the one-time pad (OTP). The key should be used only once and be as long as the message to be sent. The efficient distribution of such long keys remains an issue. Quantum key distribution (QKD) provides a means to deliver key material for OTP over an optical network. Experimental demonstrations and development of QKD were carried out by many research institutes in the 1990s. In the 2000s QKD systems were transferred from the controlled environment of laboratories into a real-world environment for practical use. Progress has also been made in theory, not only developing new tools to prove protocols themselves but also analyzing the security of practical QKD systems. The commercialization of QKD has also been successful.

In the past decade, multi-user QKD networks have been extensively investigated in field environments. The DARPA Quantum Network, as part of a project supported by the US Defense Advanced Research Projects Agency (DARPA), pioneered the deployment of QKD in a field network. The network consists of 10 nodes linked together through an actively switched optical network. The European FP6 project Secure Communication using Quantum Cryptography (SECOQC) integrated a number of different QKD systems into one quantum backbone (QBB) network, developing a cross-platform interface. From the SECOQC project, the European Telecommunications Standards Institute (ETSI) industry specification group for QKD (ISG-QKD) was launched to offer a forum for creating universally accepted QKD standards. Long-term QKD operation also has been tested in a field environment, such as the Swiss Quantum network in Geneva the Durban network in South Africa developed by the Durban–Quantum City project and the Cambridge Network. Transparent network implementations of QKD have been demonstrated, such as a dynamically reconfigurable network in a testbed of the Advanced Technology Demonstration Network (ATDNet) in the Washington D.C. area by Telcordia Technologies, a passive optical network consisting of core ring and access network in Madrid by Universidad Politécnica de Madrid and Telefónica Investigación y Desarrollo, a hierarchical network consisting of a 5-node wavelength division multiplexing (WDM) quantum backbone and subnets connected by trusted nodes, in Wuhu, Anhui, by one group from the University of Science and Technology of China, and an all-pass optical switching network in Hefei, Anhui, by another group from the same university.

All these QKD field trials adopted either or both of the following two kinds of networking schemes: key relay via trusted nodes, and transparent link via optical switching. The former requires guaranteed physical security of the relay nodes, but can expand key distribution distance arbitrarily. The latter can realize key establishment for many users with less complexity of key management over an untrusted network. The distance and the secure key rate are, however, limited by an overall optical loss. Which networking scheme is mainly used depends on the purpose and the infrastructure to be installed.

To appeal to a wider adoption of QKD, it is indispensable to demonstrate applications demanded by potential users of high-end security technology, such as secure TV conferencing, and secure mobile phone in an area as wide as possible. The typical QKD link performance in the field networks so far was represented by the secure key rate of a few kbps at a distance of a few tens of km, which was only sufficient to encrypt voice data by real time OTP, or to feed the primary session key to a classical encryptor. The secure key rate needs to be significantly improved for other applications. To expand the QKD distance, currently one needs to rely on a key relay via trusted nodes. In this paper, we present a metropolitan QKD network with trusted nodes, called the Tokyo QKD Network, where the latest QKD technologies and an upgraded application interface were installed, and various applications including secure TV conferencing and secure mobile telephony were demonstrated. Novel QKD technologies that enabled the world-first demonstration of OTP encryption of movie data over 45km field fibers are explained.

In the communication layer, secure communication is ensured by using the distributed keys for encryption and decryption of text, audio or video data produced by various applications. Users are within the trusted nodes. User data are sent to KMAs, and encrypted and decrypted by OTP in a stored key mode. Beside OTP-encryption, Advanced Encryption Standard (AES) is also implemented in each KMA. The KMS switches two cryptographic schemes, referring residual amounts of secure keys. The centralized management by the KMS differentiates the Tokyo QKD Network from the SECOQC network. In the latter, the secure path-finding problem is solved by an autonomous search algorithm following standard approaches in networking. The main reason for adopting the centralized management in the Tokyo QKD Network is that it assumes a test case of a government-chartered network or a mission critical infrastructure network which often have a central dispatcher or a central data sever. In particular, we examine a point-to-point link as the very first test case. In our current mesh type network, there are limited number of relay routes. So the routing algorithm is simple, i.e. the KMS organizes a routing table for end points which have been requested by users, and then selects an appropriate route from it.

The physical implementation of the three-layer architecture is depicted by the wiring diagram in Fig. The blue lines represent optical fibers for the quantum layer. For links no. 1, 3, 5 and 6 a second fiber was used to send the classical information required for the QKD protocol and synchronization signals, according to the original specification of the Tokyo QKD network. On the other hand, for links 2 and 4, the synchronization signal was sent through the same fiber the classical signals required for QKD were sent through a different fiber, shown as a different color in Fig. All the KMAs are located inside the network isolated from each other by L2 switches. The network itself is connected to the Internet via a router.

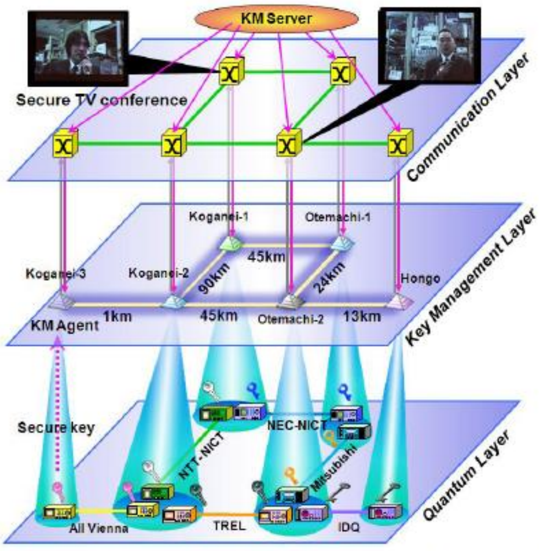

Fig. 2. Three-layer architecture of the Tokyo QKD Network. It consists of the quantum, t management, and the communication layer.

QKD systems used in the Tokyo QKD Network

The performance of QKD has been much improved in recent years owing to the progress in state-of-art technologies, such as novel photon detectors operating at higher speed with lower noise and faster electronics. In the Tokyo QKD Network, high speed QKD systems developed by NEC-NICT and TREL have enabled real-time secure video conferencing in a metropolitan area. The DPS-QKD system developed by NTT allows for real-time long-distance secure voice communication. Mitsubishi combined its QKD system with an application for secure telephony over smartphones. A reliable and highly stable commercial system was demonstrated by IDQ. Finally, All Vienna contributed with an impressive next-generation QKD system using quantum entanglement.

NEC and NICT developed a one-way decoy-state BB84 system, aiming at fast QKD for metropolitan-scale distances, which can realize OTP encryption of video data. The system is designed for a multi-channel QKD scheme with wavelength division multiplexing (WDM). Each channel is operated at a clock rate of 1.25 GHz. A block diagram of the QKD system is depicted in Fig. 4. The upper part shows the optical transmission block and the lower part represents the key distillation block, where a dedicated hardware engine is used for the key distillation process. The hardware engine has a large memory, large-size field programmable gate arrays (FPGAs), and high speed in/out interfaces, which can potentially handle up to 8 WDM channels, i.e. for a processing speed of up to 10Gbps.

A dual-drive Mach-Zehnder modulator produces four quantum states in the time-bin encoding, according to pseudorandom numbers provided by a controller. (In future, true random numbers should be used. An interface for ultra-fast true random number generators has already been equipped in the system.) The quantum signal is combined with the clock and frame synchronization signals by a WDM coupler, and these multiplexed signals are transmitted through the same fiber for precise and automatic synchronization. The crosstalk between quantum and classical channels in the same fiber is suppressed by appropriate wavelength allocation and placing narrow bandpass filter at the receiver.
In the receiver, the quantum and the synchronization signals are divided by a WDM filter. The quantum signal is discriminated by a 2-by-4 asymmetric and totally passive PLC-MZI, and is then detected by a four-channel SSPD, which is free from the afterpulse effect and complex gate timing control. The detection efficiency and the dark count rate of the SSPD itself are about 15% and 100 cps, respectively. When it is combined with the QKD system, however, the total detection efficiency reduces to about 7%, and the noise count rate increases to 500 cps due to stray light. The reduction of the total detection efficiency is due to that the active time window imposed on the time-bin signal cannot cover the whole pulse spreading after the fiber transmission. The active time window can assures the simultaneous photon detection for all the SSPDs, enhancing the uniformity of the detection efficiency of each detector.[1]

Quantum repeaters enable entanglement distribution between remote parties by relying on a network of quantum memory units. In their seminal paper, Briegel et al. demonstrate how to distribute entanglement over arbitrarily long distances using ideal quantum memories as well as highly efficient quantum gates for entanglement purification. The resources needed in such a scenario will then only grow polynomially with distance for a fixed desired fidelity for the final entangled state.

Further studies have shown that so long as the coherence time c of the memories is much longer than the transmission delay L/c, where L is the distance between the two parties and c is the speed of light in the channel, the above assertion still holds. It is not clear, however, how the required resources scale in the limit of large distances when c is finite. Here, we answer this question by assuming that the only error-correction mechanism used in the system is entanglement purification in conjunction with allowing for error-free, but probabilistic, gates to be used instead of erroneous deterministic ones. We find that, even under optimistic assumptions, the system cost explodes as a power, unless we employ a fault-tolerant scheme to remedy the memory decay.

In order to quantitatively address the cost factor in quantum repeaters, we look at the generation rate of maximally entangled states per employed memory in the system. We employ proper entanglement measures, instead of merely looking at the fidelity, to find this rate. We obtain this rate, in the steady state, assuming that the resources in our system are being successively used, according to a proper protocol, to create entangled states. Such a rate-over-cost measure is useful for applications in quantum key distribution (QKD), where the generation rate of secure key bits is proportional to the rate of entanglement generation. Moreover, it provides us with a fair and practical measure for comparing different quantum repeater setups and their contrast with alternative schemes for entanglement distribution that do not rely on using quantum memories, such as quantum relay structures or the direct transmission of entangled photons. In the latter cases, the rate will decay exponentially with distance as a result of loss in the channel.

Memory decay is one of the most challenging problems in quantum repeater technology. Its deteriorating effect, however, has not yet fully scrutinized. In authors study the role of memory errors in quantum repeaters, but they treat the required initial entanglement as a given resource. This approach cannot fully capture the memory decay problem as it neglects to account for the corresponding waiting times during initial entanglement distribution.

Entanglement distribution, regardless of the employed scheme, is a probabilistic process, mainly because of its dealing with the loss in the channel, and therefore, the time required to entangle two memories is a random variable. Collins et al. consider this probabilistic nature in a multiple-memory configuration, and report a numerical-analytical rate analysis that includes the effects of memory decay. They model the memory decay by associating a lifetime window within which the stored entanglement is unaffected and beyond which it is destroyed to each memory. This simple model is not, however, sufficiently realistic to properly account for the effect of memory errors on the rate, especially in the regime of short coherence times. [2]

Over the past decade, there have been significant advances in optical networking technology that have increased the configurability and transparency of fibre networks. A key enabler of this evolution has been the successful development and wide deployment of the reconfigurable optical add drop multiplexer (ROADM) in core, metro and access networks. ROADMs move fundamental networking functions such as multiplexing and routing from the electronic domain to the optical domain. The resulting optical transparency permits the transport of high speed communications signals using advanced optical modulation formats without requiring intermediate nodes to be upgraded. It also opens up the prospect of supporting even more exotic optical signals, such as photonic qubits for quantum communications. The most mature quantum communications protocol, quantum key distribution (QKD), offers the possibility of providing a highly secure key establishment service across a network. Optical transparency removes a critical roadblock to sending quantum signals over previously opaque networks.

However, transparency does not guarantee that quantum signals can coexist with high-power classical channels on a shared network and maintain sufficient fidelity between end users to support quantum services such as QKD. While there have been several successful demonstrations of quantum technologies on optical fibre systems, many of these experiments have been performed over dedicated network infrastructures. The focus of the work described in this paper is to understand under what conditions quantum signals (e.g. those used to perform QKD) may be able to coexist with signals typically found in enterprise or metro-area telecom networks. At present, such a coexistence is a challenge as current networks may carry up to 80 classical dense wavelength division multiplexed (DWDM) channels on a 50–200 GHz frequency grid. While our previous work has demonstrated the compatibility of 1310 nm QKD with strong classical 1550 nm DWDM communications channels, there may be advantages in placing the QKD signals in the same low-

loss 1550 nm transmission window with the classical signals. Potential advantages include increased signal reach for QKD and compatibility with infrastructure not transparent to or already occupied by 1310 nm signals. However, decreasing
the wavelength spacing between quantum and classical signals substantially increases the background noise, placing more stringent demands on filtering.

A first demonstration of 1550 nm-based QKD with a single in-band classical DWDM signal was reported, where the quantum and classical signals were spaced by either 400 or 800 GHz. The networking architecture assumed a static, point-to-point connection between a single QKD transmitter and a single QKD receiver. The authors of conclude that the dominant impairment impacting QKD performance in their experiment was inadequate filter isolation of the single classical channel. Although their paper was an important first step, we improve on their results in several important ways. First, we demonstrate sufficient filter isolation (>110 dB) to overcome the classical channel crosstalk found. Here, our improvements enable the use of 200 GHz channel spacing and allow us to measure the transmission effects that can become fundamental limits to the coexistence of QKD with classical communications channels. Next, we explore the impact of up to two simultaneous classical channels co-propagating with the quantum channel. Finally, we remove the point to point constraint present in the previous QKD/DWDM experiments by using a ROADM network element, which has switching and multiplexing capabilities, to emulate a reconfigurable network. The addition of a ROADM network element opens up the possibility for transparent path reconfiguration between QKD endpoints, which can enable scalable quantum networking over metro-size regions without requiring secured, optical–electrical–optical-based key regeneration, which has been proposed by other groups.

Improved spectral filtering enables the identification and experimental mapping of the primary impairments to quantum signals from closely spaced co-propagating DWDM classical signals. We show that the dominant impairment can arise not only from Raman scattering as was previously shown but also from four-wave mixing (FWM). These two sources of noise can be challenging to manage since they can fall directly in the centre of a pass band intended for ultra-low power optical channels for QKD, and one cannot use simple filtering approaches to entirely reject them. However, theoretical calculations enable us to design experiments where these two impairments may be studied in relative isolation from each other. Experimentally, we explore channel spacing between the quantum and classical signals as close as 200 GHz, and theoretically, we calculate the effects of spacing as close as 10 GHz. We measure the impact of the classical signals both with a single-photon detector and with a 1550 nm QKD system, both utilizing typical ns-gated InGaAs avalanche photo-diodes (APDs).We demonstrate that the dominant noise mechanism depends on the optical path characteristics as well as the classical channel parameters, and discuss impairment mitigation strategies. [3]

Quantum cryptography [or quantum key distribution (QKD)] was the first application of the evolving field of quantum information technology to become commercially available. The maximum distance for QKD in practical applications, however, is currently limited by the noise of available single photon detectors and the absorption along the quantum channel, for example, in fiber to about 100 km. In principle, this problem can be overcome by subdividing a larger distance into smaller segments and employing a quantum repeater scheme. Yet, this is still far beyond state-of-the-art technology. In the meantime, a network of trusted nodes connected by fiber or short free-space links is one option for bridging longer distances. Alternatively, a free-space link from a lowearth-orbit (LEO) satellite to a ground station could be used. By exchanging quantum keys between the satellite and different ground stations consecutively, one can easily establish a secret key between any two ground stations worldwide, thereby enabling truly global quantum key distribution.

QKD traces its security back to the fact that it is impossible to determine the general quantum state of a single photon. Yet, compared to using sources of single or entangled photons it is technologically much simpler for the transmitter to generate attenuated laser pulses. Even for a low average photon number well below one, the Poissonian nature of the laser photon statistics opens back doors for attacks by a potential eavesdropper.

In the most powerful one, the photon number splitting (PNS) attack, the eavesdropper removes a photon from all pulses containing two or more photons and measures its state after bases are announced. In high loss situations, he obtains the full key. To avoid such leakage one has to strongly attenuate the laser pulses], approximately proportional to the link efficiency. The significantly lower key rate makes attenuated pulse QKD very unattractive or even impossible. The recently proposed decoy-state analysis enables one to detect such attacks. There, the mean photon number for secure communication becomes approximately independent of the link loss and the key rate scales equally to the single photon case. [4]

There is currently much interest in using quantum cryptography as a method for distributing cryptographic keys on fiber optic networks,1 the secrecy of which can be guaranteed by the laws of quantum mechanics. Since any information gained by an eavesdropper causes errors in the formed key, the sender (Alice) and receiver (Bob) can test its secrecy. Provided the quantum bit error rate (QBER) is less than a certain threshold,2 error correction3,4 and privacy amplification can be applied to form a perfectly shared key with minimal information known to
an eavesdropper.

Since the original proposal by Bennett and Brassard6 in 1984, quantum key distribution (QKD) systems based upon transmission of encoded weak coherent pulses have been implemented by a number of groups. The most successful approach for fiber optic based systems has been to encode the qubit information upon the phase delay in an interferometer. In the absence of a ‘quantum repeater’ which could regenerate a modulated photon, photon loss in the fiber limits the maximum distance over which quantum cryptography may be applied. As the fiber length increases, the signal rate falls to a value approaching that of the intrinsic error rate of the receiver’s equipment. Eventually this results in the QBER exceeding the threshold for privacy amplification, preventing a secure key from being formed. Until now this has restricted demonstrations of QKD to fiber lengths shorter than 100 km. We show here that this barrier can be exceeded by minimising the contribution to the intrinsic error rate of detector dark count noise
and stray photons. With some improvements distances up to 165 km could be possible.

Our system is based upon a time division Mach-Zender interferometer using phase modulation, Polarising beam combiner and splitter are used so that photons from Alice’s short arm are directed into Bob’s long arm (S-L) and vice versa (L-S). The lengths of two routes S-L and L-S are roughly matched using a variable delay line in Alice’s setup, with fine adjustment achieved by using a fiber stretcher in Bob’s long arm. Thus the relative phase delays introduced to the two paths by Alice and Bob using their phase modulators, determine the probability that a photon exits either output of Bob's interferometer.

Photons are generated by a 1.55 μm distributed feedback pulsed laser diode operating at 2 MHz with a pulse width of 80 ps. The pulses are strongly attenuated so that on average 0.1 photons per clock cycle leaves Alice's apparatus. The intensity ratio of the reference pulse (though Alice's long arm) to the encoded pulse (through Alice's short arm) is 1.6:1, so that the encoded signal contains 0.04 photons per pulse on average. Phase modulators controlled by custom electronics, in the two interfering routes are used to encode the bit information. The signal is multiplexed with pulses from a 1.3 μm clock laser which serves as a timing reference. InGaAs avalanche photodiodes operating in gated mode, with a gate width of 3.5 ns and an excess voltage of 2.5 V, and cooled to an approximate temperature of -100 ºC, are used to detect the single photons. It is imperative for operation over long fibers that the dark count rate in the single photon detector is as low as possible. Our detectors typically have a dark count probability of 10-7 per ns, along with a detection efficiency of around 12% at 1.55 μm. This corresponds to a Noise Equivalent Power of 1.1×10-17WHz-1/2, which is one of the lowest reported to date at this operating temperature.

The quantum interference fringe visibility is greater than 99% for lengths up to 65 km and decreases for longer fiber lengths. Beyond 65 km, the fiber attenuation reduces the signal rate to a value comparable to the intrinsic error rate in Bob's detector. Nevertheless, by minimising the intrinsic error rate, we have achieved a visibility of 88.4% at 122 km. There are two major contributions to the intrinsic error rate which limits the visibility. (As we discuss later, a third source of errors also contributes to the QBER.) These are, firstly, the dark count noise of the detector, and, secondly, stray light from the intense clock laser which is not fully filtered by the wavelength-division multiplexing (WDM) filter. The probability of an error count per clock cycle (*Pe*) was measured to be 8.5x10-7. Of this, the probability of a detector dark count in the 3.5 ns gate was measured to be 3.2x10-7. This shows that the contribution from stray light dominates over that due to the detector dark count, suggesting that the visibility (and QBER) could be improved by stronger filtering of the clock laser. [5]

QKD, the most mature quantum cryptography technology, has attracted much attention in the past five years as data security becomes much more important than before. Unlike other popular cryptography technologies based on computational complexity, quantum cryptography relies on the randomness generated by Mother Nature. Because of its quantum nature, QKD is unbreachable, no matter how advanced the computer algorithms and hardware. QKD is attractive for deployment in both local area as well as large scale carrier networks because it provides the ultimate security for optical communications.

Since QKD utilizes about one photon for each bit in the quantum transmission channel, the intensity of the quantum channel is much lower than that of a normal data channel. For example, if exactly one photon per bit is used, the average power of a 1 Mbps quantum channel is about -100 dBm (for 1550 nm). Moreover, when attenuated laser pulses are used for QKD, the average number of photons per pulse needs to be decreased below one to reduce the possibility of photon splitting attacks. Thus, the average power in the quantum channel drops even further. If the power of a data channel is -10 dBm, the difference between the quantum channel and the data channel can be over 90 dB. Therefore, a quantum channel usually is carried by a dedicated fiber not polluted by the data carrying channels.

However, carrying the quantum channel and the data channels on the same fiber is an attractive solution as it eliminates the end user's burden to reserve a separated fiber for each quantum channel. To realize this, we have to study the impact of elastic and inelastic effects from the data channels to the quantum channel. The elastic effects include Rayleigh scattering, cross-talk and directivity of multiplexer and demultiplexer, and the inelastic effect of Raman scattering. The impact of Rayleigh scattering and Raman scattering has been studied thoroughly in previous work. To reduce the effect of Raman scattering, the quantum channel should be placed at the shorter wavelength side related to data channels, because anti-Stocks spectrum is much weaker than Stocks spectrum. It is probably the reason that in Ref. 4 a 1310 nm channel is used for the quantum channel while the data channels stay in 1.5 um band, far away from the quantum channel. This large wavelength separation may reduce the cross-talk mentioned above. In this work we studied a topology in which both the quantum channel and the data channels are carried by the C-band wavelengths. Compared to previous work, the wavelength separation of the quantum channel and the data channels is much smaller, which helps us better understand the impact of the data channels. The transmission distance was doubled in this work (as compared to the earlier experiments), resulting in a more practical 50 km span. To our knowledge, this is a first experimental demonstration of a practical deployment of a QKD link on the fiber populated by in-band classical data channels. [6]

Quantum key distribution (QKD) is a promising candidate for next-generation security networks. Recently, some point-to-point QKD realizations have been successfully operated in telecommunication dark fibers, while many groups are aiming at practical quantum cryptography networks. Several QKD local network topologies have been proposed with the optical method. In this letter, we focus on a star topology QKD network based on wavelength-division multiplexing (WDM), applying it to a four-user system built in the commercial backbone telecommunication fiber network of China Netcom Company Ltd. (CNC) in Beijing in March 2007. The router in the center of the network performs network addressing according to the wavelength of the quantum signal and the specific connection of the WDM inside it. The transmitter can actively select the key transfer destination by choosing the corresponding wavelength, which is different from a network composed of passive optical splitters. According to this topology, a user can directly exchange quantum keys with any other user without the need for trusted relays, and all users are equivalent in this topology.

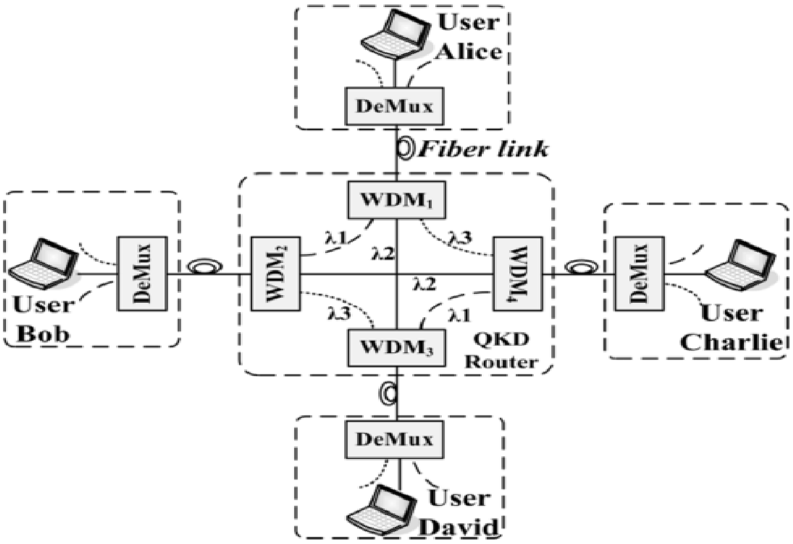

Fig. 1. Structure of four-user QKD router and the star network topology. DeMux: demultiplexer.

Topology of Multiuser QKD Network

As an example, a four-user QKD network is used to describe the topology. The router is composed of three-wavelength WDMs. When Alice wants to send a quantum signal to Bob, she selects wavelength corresponding to the specific connection inside the router, as shown in Fig. 1. These photons will be demultiplexed by WDM and transmitted to WDM through the link between WDM and WDM , then forwarded to Bob. Alice can transmit photons of , , and at the same time in principle; then she can exchange keys with Bob, David, and Charlie simultaneously, although the cost will increase. The operations of all the other users are the same as for Alice. Since only two WDMs are added into the QKD links, any point-to-point QKD realizations can be used in this network architecture. However, the maximum secure transmission distance will be reduced a little due to the additional insertion loss. [7]

The ultimate usefulness of most communications services depends strongly on the ability to network, i.e., to efficiently connect many end users with each other or with shared resources. Much of the experimental research on Quantum Key Distribution (QKD) has focused on improving transmission performance over a fixed end-to-end connection between a single pair of quantum endpoints, Alice and Bob. However, this type of connectivity does not scale well, because the level of resources that are required increases very rapidly with the number of end users. Efficient networking solutions are clearly needed to move QKD and other types of quantum communications beyond the realm of niche deployments.

Many of the technologies, components and techniques needed to address these problems have been developed over the past quarter century for use in conventional optical fibre networks. Early fibre networks utilized optics solely for point-to-point (PTP) transmission between opaque nodes, in which all networking functions were implemented electronically. In contrast, modern fibre networks increasingly take advantage of optical transparency, in which a subset of critical networking functions such as switching, routing and multiplexing are preferentially performed in the optical layer. This enables the establishment of multiple optically transparent lightpaths through a network domain, and highly dynamic re-routing or reconfiguration of these lightpaths.

Applied to QKD, optical networking offers the prospect of flexible and scalable on demand connectivity for a large number of Alice-Bob pairs. End-to-end key establishment over an untrusted network is feasible for lightpaths compatible with the maximum attenuation allowed by the QKD system. Communications over longer end-to-end paths, or between endpoints with incompatible QKD systems, can be routed on demand via a shared set of 'trusted relay' nodes in secured locations. The network can also provide endpoints with optically transparent access to other shared resources, such as 'centralized' entangled-photon sources for QKD. Finally, optical networking offers the prospect of leveraging costly infrastructure already deployed for telecom and enterprise networks, via wavelength-division multiplexing (WDM) of quantum and conventional data signals onto the same fibres. A central question for the future of QKD is to what extent it can attain wide applicability by taking advantage of these major advances in conventional optical networking.

Achieving this vision requires developing new capabilities, and validating them in realistic network environments. In this paper, we experimentally demonstrate a number of fundamental capabilities of optical networking as applied to QKD. These include optical routing, automated restoration after network path reconfiguration, and multiplexing and transmission of QKD with strong conventional WDM channels on the same fibre. We also examine practical considerations for applying optical networking architectures and technologies to QKD, and resulting impacts on the quantum signals in these environments. Although the experiments and analyses reported in this paper focus entirely on QKD, many of the results are likely to also carry implications for a broader range of quantum communications services which rely on the transport of photonic qubits over fibre networks.

The earliest QKD optical networking experiments were reported by Townsend's group, which measured quantum bit error rates (QBER) for QKD signals transmitted through a 1:3 passive optical splitter to facilitate distribution of QKD signals to three different receivers. Following this work, several additional groups proposed passive fibre distribution networks to transmit key to multiple nodes. Our group reported the first demonstrations of QKD through optical switches, including key establishment through several types of switch fabrics, and optical protection switching between two fibre paths connecting Alice and Bob. Honjo et al. used a planar lightwave circuit (PLC) switch to connect Alice with either of two Bobs, demonstrating low QBER in the presence of crosstalk from a much stronger channel on a different path through the switch. Optical switching has also been used in a portion of the DARPA quantum network, and investigated in a three-node QKD configuration at NIST.

The Role of Optical Networking in Quantum Communications

The value of communications depends strongly on the number and variety of endpoints that are accessible. For example, for peer-to-peer applications such as voice calls, file transfers, or QKD sessions between a pair of end users, Metcalfe's Law suggests that the value of the service is roughly proportional to the square of the number of users that can be interconnected. The value of shared resources on a network such as Web servers, key servers, or entangled photon sources, also depends strongly on the number and variety of end users to which access can be provided.

Optical fibre is the most practical way to reach a large number of endpoints, whether end users or servers; however, static PTP fibre connections are not scalable to large numbers of endpoints. Efficiently interconnecting these endpoints is an optical networking problem. Quantum communications can take advantage of the technologies, components and architectures developed over the past two decades for conventional fibre communications. Figure 1 provides a schematic overview of two different types of reconfigurable quantum communications networks. The boxes labelled A and B represent quantum endpoints (Alices and Bobs) at a variety of locations. The cloud on the left represents a network domain dedicated entirely to quantum-based services. (In addition to quantum signals, this network might also carry a small number of directly related classical signals, e.g. the 'public' reconciliation channels for QKD.) The cloud on the right represents a shared network domain, in which quantum channels are wavelength multiplexed onto fibres carrying conventional optical data traffic in a typical large telecom (carrier) or enterprise (private business) network. Within each of the two clouds, the endpoints are interconnected by a mesh of optical routers. These could be simple fibre switches, wavelength-selective switches, or other existing devices capable of independently routing wavelengths through the node. An important point is that these routers are optically transparent, and do not themselves originate or terminate quantum signals. The quantum signals are transmitted transparently end-to-end between Alice and Bob. As a result, the optical routers themselves need not be trusted or physically secured.

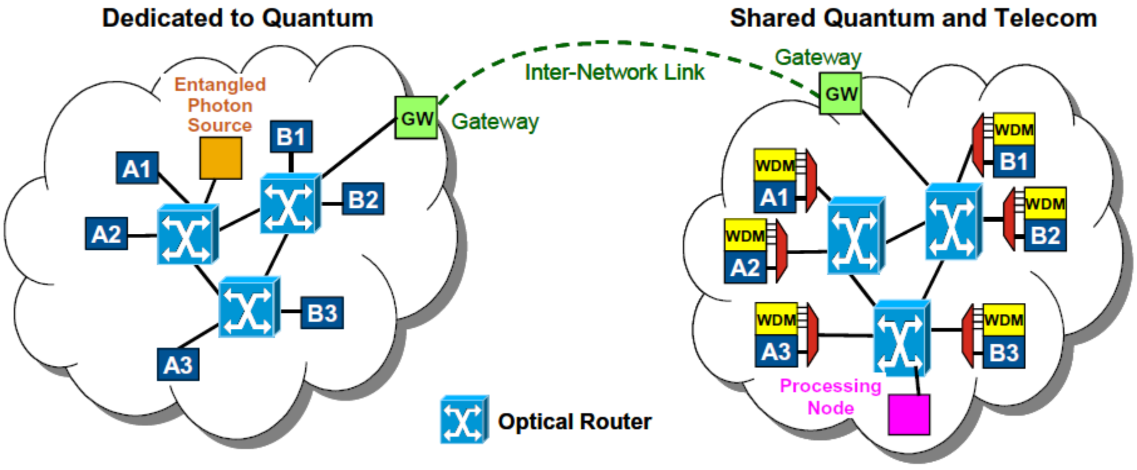

Figure 1. Schematic view of two types of reconfigurable optical network domains. See text for discussion.

Within each network domain, the optical layer provides some of the *networking* functionality, rather than simply PTP *transmission* as in the trusted relay model. The optical routing and multiplexing are electronically controlled, and can be dynamically reconfigured as needed. This provides flexible, optical layer on-demand connectivity between any Alice and any Bob in the domain (within the range limitations of the quantum signals for the particular service being provided, e.g., QKD). It also avoids the scalability problems associated with dedicated connections for every Alice-Bob pair. In addition, reliability is enhanced by the ability to optically reroute signals along alternate paths in the case of network failures, congestion, or high error rates due for example to noise or other interference.

Optical-layer reconfigurability also provides end users with transparent access to shared resources, such as 'centralized' entangled photon sources for on-demand entanglement-based QKD. Processing nodes, including trusted relays, can similarly be placed on the network and accessed on an as needed basis, for example to extend QKD range or to interface between incompatible quantum transmission systems.. It has been correctly stated that transparent optical networks do not increase the range of QKD, and in fact decrease it somewhat due to attenuation in the additional optical components required for networking functionality. However, the choice is not restricted to fully transparent networks versus fully opaque networks. Modern fibre networks utilize a judicious combination of transparent networking and shared intermediate nodes (e.g., digital regenerators for classical optical signals). This hybridized approach has the potential to significantly reduce the number of opaque nodes required, along with the associated cost, complexity, and potential security requirements.

Large communications networks are almost invariably constructed from sub-networks or administrative domains, for reasons of scalability and manageability. A limited number of gateways in each domain are used for interconnection and routing of traffic among the various domains. Optical reconfigurability between endpoints and gateways supports efficient aggregation of traffic headed for other domains (e.g., over the internetwork link in figure 1), and efficient distribution of traffic upon its arrival. This hierarchical approach is characteristic of communications networks, with different architectures and technologies in the access, metro, and core (long-haul) regimes, driven by different distance scales, traffic patterns, and cost considerations. In the quantum realm, for example, inter-network links could involve different types of fibre-based implementations, chains of quantum repeaters, or free-space links. Gateways provide the necessary adaptations, and often play an important role in securing communications entering or leaving a domain. For these reasons, gateways are natural locations for secured opaque processing nodes needed to support quantum services.[8]

4. Conclusion

In this paper, well-known techniques in classical multiple access optical communications were applied to quantum cryptography applications. That enabled multiple users to exchange secret keys, via an optical network, without trusting any other nodes. The proposed setups offered key features that would facilitate their deployment in practice. In all of them, classical communications services were integrated with that of quantum on a shared platform, which would substantially reduce the cost for public and private users. More generally, by sharing network resources among many users, the total cost per user would shrink, making the deployment of such systems more feasible. Another cost-saving feature in our setups was their relying on only one QKD detection module per user. The setups considered were inspired by existing optical access networks as well as future all-optical networks. A passive starcoupler network was first studied when multiple QKD users could pair up and simultaneously exchange secret keys via the network. Each user could independently use classical communications as well. Different users could be distinguished in time, using a TDMA scheme, or in the code space using OOC CDMA. It turned out that, whereas TDMA QKD could offer an interference free, or, effectively, a point-to-point QKD service, CDMA QKD should deal with the interference effect. It was shown that the optimal performance for a CDMA QKD system could be achieved if codes with weight one were used, for which interference probability would be minimum. In this case, the encoded CDMA signal was somehow similar to the TDMA one, except that no time coordination was needed between all network users. To enjoy the benefits of both TDMA and CDMA systems, a listen-before-send protocol was proposed, whose performance could approach the TDMA QKD once the number of listening periods was sufficiently large. To support a larger number of users, hybrid WDMTDMA CDMA architectures, potentially compatible to future all-optical networks and PON access systems, were proposed and their performance in terms of secret key generation rates and numbers of users was studied.

References

[1] Mohsen Razavi, " Multiple-Access. Quantum Key Distribution Networks", vol. 60, ISSN :0090-6778, July 2012.

[2] C. H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” in *Proc. 1984 IEEE International Conf. Comput., Syst., Signal Process.*, pp. 175–179.

[3] P. W. Shor and J. Preskill, “Simple proof of security of the BB84 quantum key distribution protocol,” *Phys. Rev. Lett.*, vol. 85, no. 2, p.441, July 2000.

[4] H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” *Phys. Rev. Lett.*, vol. 94, p. 230504, June 2005.

[5] C. Gobby, Z. L. Yuan, and A. J. Shields, “Quantum key distribution over 122 km of standard telecom fiber,” *Appl. Phys. Lett.*, vol. 84, pp. 3762–3764, 2004.

[6] T. Schmitt-Manderbach *et al.*, “Experimental demonstration of free-space decoy-state quantum key distribution over 144 km,” *Phys. Rev. Lett.*, vol. 98, p. 010504, 2007.

[7] S. Wang *et al.*, “2 GHz clock quantum key distribution over 260 km of standard telecom fiber,” *Opt. Lett.*, vol. 37, no. 6, pp. 1008–1010, Mar. 2012.

[8] Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, “Practical gigahertz quantum key distribution based on avalanche photodiodes,” *New J. Phys.*, vol. 11, p. 045019, Apr. 2009.

[9] K.-I. Yoshino *et al.*, “High-speed wavelength-division multiplexing quantum key distribution system,” *Opt. Lett.*, vol. 37, no. 2, pp. 223–225, Jan. 2012.

[10] H.-J. Briegel, W. D¨ur, J. I. Cirac, and P. Zoller, “Quantum repeaters: the role of imperfect local operations in quantum communication,” *Phys. Rev. Lett.*, vol. 81, no. 26, pp. 5932–5935, Dec. 1998.

Authors' Biography

Md Sarwar Pasha had B.Tech from Syed Hashim College of Science and Technology, Pregnapur, Medak District. He is an M.Tech. student in CSE Department of CMR Institute of Technology, Hyderabad. He is currently doing his M.Tech. Project work under the guidance of **Mr.A.Bala Ram.**

Mr. A. Bala Ram, He is currently working as Associate Professor in CSE Department of CMR Institute of Technology, Hyderabad. His areas of interest are Net work security, cloud computing, image processing.