I. J. Computer Network and Information Security, **2012, 6, 43-48**
Published Online June 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.06.06

Multi-User Quantum Key Distribution Using Wavelength Division Multiplexing

P. Lokesh Kumar Reddy[1], B. Rama Bhupal Reddy[2], S. Rama Krishna[3]

[1]Assistant Professor, Department of Computer Science,
Rama Raja Institute of Technology and Science, Tirupati, A.P., India.

[2]Associate Professor, Dept. of Mathematics, K.S.R.M. College of Engineering, Kadapa, A.P., India.
reddybrb@gmail.com

[3]Professor, Dept. of Computer Science, S.V. University, Tirupati, A.P., India.

***Abstract* —** Quantum cryptography, exclusively known as Quantum key distribution (QKD), has attracted a lot of attention in the recent years with the discovery that it can provide absolute secrecy for communications. We report a new architecture for constructing a fiber-based network of quantum key distribution using optical wavelength division multiplexing in the fiber, and also using some wavelength protocols. The advantages are discussed in detail for demonstrating the experimental report in the way of feasibility for the proposed architecture.

***Index Terms*—**Quantum Cryptography, Quantum Network, Wavelength Division Multiplexing

I. INTRODUCTION

Confidentiality of communication between two legitimate parties can now-a-days have a paramount importance that will inevitably grow larger in the future. Solutions offered by classical cryptography are either secure but impractical to implement, or practical and lack a proof of security [1]. The BB84 protocol for Quantum Key distribution (QKD), can overcome the difficulties of both classical solutions by providing a way to securely generate arbitrarily long cryptographic keys using the quantum properties of light. The intuition behind the principle is rooted in two fundamental aspects of quantum properties of light. The intuition behind the principle is rooted in two fundamental aspects of quantum mechanics, which are the no-cloning theorem[2] and the uncertainty principle that states that one cannot measure an arbitrary quantum state without introducing a probability of spoiling it irreversibly[3]. The former thus prevents an eavesdropper to copy the key information, and the latter prevents eavesdropping without being detected, so the advantage over the classical protocols is two-fold[4].

In the BB84 protocol, two participants, Alice and Bob, wish to generate a random key using a non-confidential but authenticated fiber optic link. To do so, Alice first prepares and sends a single photon with polarization randomly chosen among the four following states: {| ↔i, | l i, | %i, | &-i}, which respectively correspond to horizontal, vertical, +45◦ and -45◦ polarization angles. Bob then analyzes the photon polarization either in the rectilinear basis, Br, where |↔i and | l i can be unambiguously distinguished, or in the diagonal basis, Bd, where | %i and | &-i can be distinguished. The result of Bob is thus deterministic when the measurement has been performed in the same basis as the preparation, in which case the result can be used as a sifted key bit. Otherwise, the result is completely random and is discarded. In the presence of errors, and possibly eavesdropping, they also need to go through classical error correction and privacy amplification protocols to eliminate key errors and to reduce the eavesdropper information about the key[6].

II. AIM OF QUANTUM CRYPTOGRAPHY

Several groups have reported the construction of fiber-based QKD systems using the BB84 Protocol at a wavelength near 1550 nm [5–9]. Fiber is the nature choice for long distance QKD because of its low attenuation and guiding properties. Also, it is not mandatory to use true singe-photon sources which are very difficult to build; coherent laser sources with a mean number of photons per time slot, μ, typically around 0.1 (assuming poissonian statistics) can be sufficient to guarantee security(i.e. to eliminate multi-photon pulses) [10-12]. Also, because of random fluctuation of fiber birefringence, polarization cannot be used without an active tracking system which makes the system inconvenient and reduces the key generation rate which is the figure of merit of QKD systems.

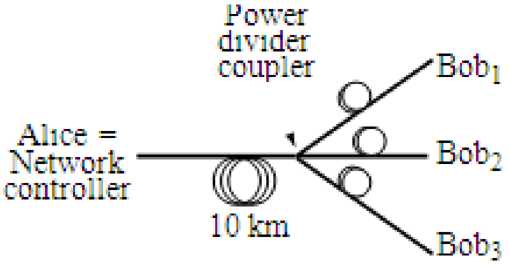

Figure 1. Townsend's multi-user set-up using a power fiber optic divider coupler.

A better choice is to encode and measure the information using the phase of the photons by carefully implementing a long-delay Mach-Zehnder interferometer [13]. However this solution, proposed by Bennett [13] and implemented by the group of R. Huges at LANL [8], requires sensitive alignment and temperature stabilization of Alice's and Bob's set-ups. To overcome this oversensitivity, the group of N. Gisin from U. of Geneva found a clever way to use an arrangement of a Faraday mirror and a polarizing beam-splitter to implement a set-up that automatically compensates for birefringence and phase fluctuations in the system, and that does not require alignment. The major problem is that it cannot be used with true single photon sources, which makes it more sensible to eavesdropping [10]. Nevertheless, their system (called the Plug and Play set-up) is proven secure against an eavesdropper with actual or near-future technology [11]. It is also easier to implement and the best choice so far.

The main content of this is organized due to the terms of security that maintains discretion by the third persons so that it is exclusively dedicated and named it as Quantum Key Distribution.

Despite the tremendous progress in two-user implementations, the development of efficient optical networks that can allow classical and quantum communication for secure data transmission is still in its early stages. We propose a new architecture for implementing a fiber-based network of quantum key distribution using optical wavelength division multiplexing (WDM). The paper is divided into the following sections. First, we show how WDM enables the creation of a local optical network in which any pair of users can communicate in a secure fashion through a trusted relay using non-entangled QKD. To demonstrate the feasibility of the proposed architecture, we report on a four-user network proof-of-principle experiment. Then, we discuss the possibility of using wavelength-tunable entanglement to build a local network that cannot be subverted by an untrustworthy relay. Finally, in a global network made up of several local networks, we show how the use of entangled QKD can reduce by half the number of relays that need be trusted.

III. FACTORS OF MUTI-USER DESIGN

In order to ever become in widespread use, QKD must be usable on networks of many users. Present technology prevents us from using fiber-based protocols on distances larger than approximately 85 km, where the noise of the detectors becomes the dominant source of errors [14]. This limits to use of QKD networks to short to medium range communication, such as a high security building or a large metro area.

Two groups investigated network architectures for QKD. The first is the group of P. Townsend (then at British Telecom) [15]. They established a passive optical network where one Alice, the network controller, is connected to multiple users (multiple Bobs). The goal is for Alice to generate a verifiably secure and unique key with each Bob using a 1 to 3 fiber power divider coupler (see Figure 1). This implies that the manager has to be trusted since he knows all the keys.

IV. SCENARIO ANAYSIS

Because of their quantum behavior, each photon is routed to one and only one user at a time and the path choice is made randomly. This scheme is inefficient since the controller cannot address each user deterministically; thereby inevitably wasting several photons as soon as one or more path are not used. Also, since the losses are important from the user to the controller, the Plug Play set-up cannot be used here since it requires backward single-photon communication [9]. The key generation rate per user, k, here goes as k_1/N , where N is the number of users and k_1 is the key generation rate with N=1. Implementing this kind of network would require important changes to the actual telecommunication infrastructure, a problem that a group from BBN Technologies (Boston) is trying to overcome by adapting the IPSEC protocol to include QKD information [16]. For long distances, they are proposing the use of trusted relays at every 50 km or so, which after all also would require important changes to the network. Their solution is however appealing for spanning a network over a city, but could not be efficiently implemented inside a large building, a flaw that our design could overcome.

The solution we propose makes use of wavelength division multiplexing (WDM) to overcome the inefficiencies of the Townsend architecture. Indeed, let us replace the power divider on Figure 1 by a de-multiplexer, and let the manager address each user Bob_i by using the appropriate wavelength λ_i (see Figure 2). We can easily conceive that such a unit (composed of the controller and the users) could well be integrated into an optical network of many similar units, making it possible to span a large distance. The number of users in the network is only limited by the number of sufficiently isolated optical channels that the fiber link can bear.

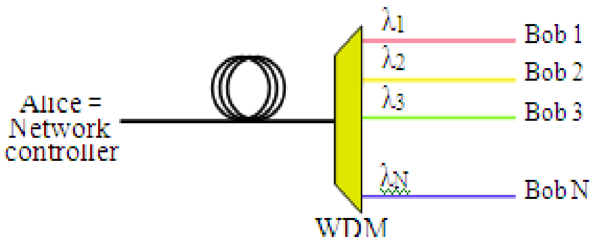

Figure 2: Multi-user design using WDM for QKD

The WDM (Wavelength Division Multiplexing) component had an isolation of 34 dB between adjacent channels and showed negligible polarization dependent loss. Therefore, only its insertion loss can affect the performance of the quantum communication when no other channels are in use. We are confident that the use of WDM components should not affect the visibility of the plug and play configuration (or other pair wise QKD configurations that don't use entanglement) over distances much longer than 10 km. However, if many channels were being used simultaneously for classical and/or quantum communication, nonlinear effects such as cross-phase modulation could spoil the crucial phase information carried by single-photon pulses. This possible limitation is under investigation by our group. Note that with the plug and play configuration, it is possible to modify slightly the relay's set-up to keep the key generation rate independent of the number of users in the network.

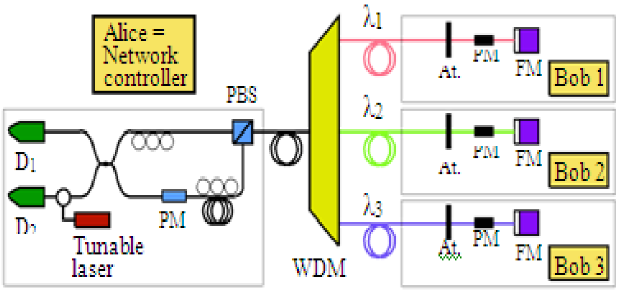

Figure 3: Multi-user design and the Plug and Play setup

Because of deterministic routing of the photons and the low losses, faint coherent pulses with μ=0.1 can be used and unlike the Townsend set-up, the Plug and Play can be implemented, making the network more efficient, easier to build and to operate. Let us show what such a network would look like with the Plug and Play set-up for pair wise key generation between the controller and each user. Figure 3 shows the controller and three users with the essential devices required (without the synchronization and detection electronics).

On the manager side, the system consists of a tunable laser, two single-photon detectors D_1 and D_2, a phase modulator PM, polarization controllers and a polarizing beam-splitter PBS. On the users side, only an attenuator At., a phase modulator and a Faraday mirror FM are required, which makes the cost of adding another user non-prohibitive. Note that only the manager is responsible for photon emission and detection, which is a clear advantage since single-photon detection at 1550 nm is technologically elaborated and can be costly to perform. The key generation rate per user k goes as k_1 $/N^0$, where N^0 is the number of used ports. Therefore, gain over the Townsend set-up is N/N^0.

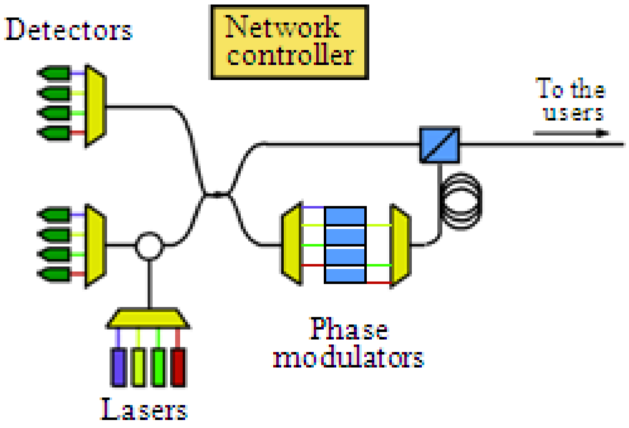

Figure 4. Modified Plug and Play set-up to keep the key generation rate per user independent of the number of users

However, with each user-end in use, the key rate per user still decreases as 1/N . One way to avoid this problem would be to send simultaneously all the wavelengths on the network. To encode different information on different wavelengths, the manager interferometer could be modified as shown on Figure 4. This way, the key rate per user could be maintained to k_1.

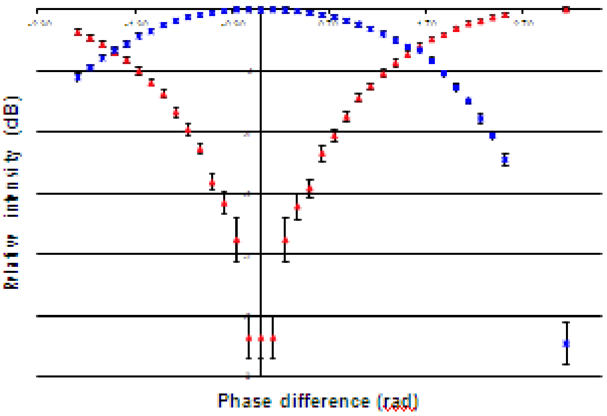

Figure 5

Figure 5. Intensity (in dB) relative to maximum output intensity in each detector as a function of phase difference at 1550.52 nm. The triangles (lower curve) and the squares (upper curve) correspond to detectors 1 and 2 respectively.

V. NETWORK USING ENTANGLEMENT

Using entangled QKD the relay need not be trusted anymore. For this, we use a wavelength-tunable source of optical entanglement that uses any degree of freedom. The key generation proceeds as follows:

1. The relay generates pairs of entangled photons at wavelengths i and j.
2. The entangled photons are sent to users U_i and U_j, through WDM (Wavelength division Multiplexing) component.
3. Users U_i and U_j are using standard quantum cryptographic methods to distil a common key k_{ij} from their shared entanglement.

Even if the relay has full control over the quantum states it sends to U_i and U_j (possibly entangling them with some local quantum probe under its control), it cannot fool them into thinking that they have succeeded in establishing a cryptographic key when, in fact, the secrecy of their key is compromised by the relay. Therefore, the relay cannot cheat or eavesdrop on the key without being caught with overwhelming probability.

On the experimental side, such a tunable source of entanglement would have to satisfy strict conditions. Among them is the need for a wide range of tunability around 1550 nm. Also, the line width of the two entangled photons should be smaller than the spacing between the WDM channels. The availability of such a source seems reasonable in the near future.

Since entangled QKD is more sensitive to losses, this reduces the maximum spanning distance of the network. However, a recent proof-of-principle experiment showed that QKD with time-bin entanglement could be realized over 50km of fiber, which would be enough for an untrusted network to be deployed over a metropolitan area.

VI. EXPERIMENTAL WORK

To demonstrate the feasibility of QKD using our proposed multi-user design, we built a network identical the one shown on Figure 3 except that it is for two Bobs instead of three. Wavelength routing was made using an ITF Optical Technologies WDM 2x2 coupler with 8 nm spaced channels aligned around 1550 and 1542 nm, and isolated by 20 dB. For optical signal generation, we used an Agilent 81689A tunable laser with a line width of 0.16 pm, modulated with a $LiNbO_3$ Mach-Zehnder intensity modulator with an on/off ratio of about 10 dB. This way, we produced pulses of about 15 ns. The coupler in Alice's apparatus has a flat response over the selected wavelengths. For phase modulation, we used LiNbO3 APE phase modulators from JDS Uniphase. Finally, for pulse detection, we used In GaAs APD EPM 239 AA SS operated in finite gain regime. The link was a 10 km spool of Corning SMF-28 single mode fiber.

We measured the visibility of interference for both wavelengths to see if the link is suitable for QKD. Note that this measurement was not made with less-than-one optical pulses, but rather with intense pulses measurable with commercially available power detectors. The disadvantage of measuring the visibility with intense pulses is to decrease the accuracy, but the mean value should be the same. In principle, if the isolation of the WDM coupler (or of any MUX/DEMUX component) is high enough, there should not be any measurable effect on the visibility as compared to the single user case (no MUX module). This indicates that the use of MUX components with 50GHz spaced channels, the smallest increment on the ITU grid*, should not cause any trouble.

In Figure 5 we can see that, at 1550.52 nm, the intensity in each detector clearly show anti-correlation in phase difference. We get the same behavior at 1542.54 nm (not shown here). The visibility in dB, defined as VdB = 10 log Imax /Imin, is about 26 ± 2 dB in both arms. This is approximately the same visibility has been measured by Stuckiet et al., [9], but without WDM. So, as expected, WDM does not imposes any limitations on the use of QKD, which demonstrates the feasibility of using such components for designing optical networks that able to bear QKD protocols.

VII. RESULTS AND DISCUSSION

By Researching the Quantum analysis, each photon is serialized to only one user at a time, random interval of time, the path is selected by user.

This process is inefficient, for the controller it is difficult to address each user, due to this reason there is a wasting of photons so more paths are not utilized properly. There is a chance of miscommunication of the photons in paths. By analyzing the above report it is best to use of wavelength division multiplexing (WDM) to overcome the inefficiencies.

The number of users in network is only equal to number of isolated optical channels.

By measuring the visibility of interference for both wavelengths to see if the link is suitable for Quantum Key Distribution (QKD).

VIII. CONCLUSIONS

In this paper, we proposed an optical network design that allows a trusted network controller to easily share secret and random keys with each user of the network by using the BB84 protocol and WDM. We showed that by using the Plug and Play set-up for pair wise key generation, the cost of adding one user to the network is non- prohibitive and this would make a robust and efficient network. We experimentally demonstrated the feasibility of using WDM components without affecting the performance of QKD.

IX. FUTURE ENHANCEMENTS

The next step is to complete the QKD set-up so that the full BB84 protocol is implemented and test the system using DWDM components. We will also investigate other types of network architectures for large scale QKD, and try to design networks that will be able to bear conventional communications as well.

REFERENCES

[1] D.Stinson, Cryptography – Theory and practice, CRC press, Inc., 2000.

[2] W.K. Wootters and W.H. Zurek, “A Single quantum cannot be clonned”, Nature 299, pp.802-803,1982.

[3] Ch.H.Bennet, G. Brassard and N.D. Mermin, “Quantum Cryptography without Bell’s theorem,” phys. Rev. Lett. 68, pp.557-559, 1992.

[4] N. Gisin, G, Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography”, Rev. of Mod. Phys. 74, pp.145-192, 2002.

[5] C. Bennett, G. Brassard, J. Robert, “Privacy amplification by public discussion”, SIAM J. Comp. 17, pp. 210—229, 1988.

[6] D.Bethune, W.Risk, “Auto compensating quantum cryptography”, New J. of Physics 4, pp.42.1-42.15, 2002.

[7] R. Hughes, G. Morgan, and C. Peterson, “Quantum key distribution over a 48 km optica fiber network,” J. Modern Opt. 47, pp.533-547, 2000.

[8] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, “Quantum Key distribution over 67 km with a Plug and Play system”, New J. of Physics 4, pp. 41.1-41.8, 2002.

[9] G. Brassard, N. Lutkenhaus, T. Mor, and B.C. Sanders, “Limitations on practical quantum cryptography”, Phys. Rev. Lett. 85, pp.1330-1333, 2000.

[10] S.Felix, A. Stefanov, H Zbinden, and N. Gisin, “Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses,” J. of Mod. Optics 48, pp. 2009-2021, 2001.

[11] D. Gottesman, H. Lo, N. Ltkenhaus, J. Preskill, “Security of quantum key distribution with imperfect devices”, http://arxiv.org/abs/quant-ph/0212066

[12] Ch.H. Bennett, “Quantum cryptography using any two nonorthogonal states,” Phys. Rev. Lett. 68, pp. 3121– 3124, 1992.

[13] D. Stucki, G. Ribordy, A. Stefanov, H. Zbinden, “Photon counting for quantum key distribution with Peltier cooled In GaAs/InP APD’s”, J. of Mod. Optics 43 (2001).

[14] P.D. Townsend, “Quantum cryptography on multi-user optical fiber networks”, Nature 385, pp. 47–49, 1997.

[15] C.Eliot, “Building the quantum network”, New J. of Physics 4, pp.46.1-46.12, 2002.

Prof. Dr. S. Rama Krishna received the M.Sc., M.Phil., and Ph.D Degrees from S.V. University, Tirupati. He is working in different positions in the department of Mathematics S.V. University, Tirupati. Recently he is working as Vice-Principal and Professor, Department of Computer Science, S.V. University, Tirupati.

His research interest includes Computational Fluid Dynamics and Computer Networks and Cryptography. He has supervised a number of M.Phil. students 10, Ph.D students 10 guided and has completed supervised one Research Project.

Dr. B. Rama Bhupal Reddy received the M.Sc., & M.Phil. degree from S.V. University, Tiruapti. In 2008, he received the Ph.D. degree from S.V. University, Tirupati. He is working as Associate Professor in department of Mathematics, K.S.R.M. College of Engineering, Kadapa. His research interest include Computational Fluid Dynamics and Mathematical Methods. He has supervised 15 M.Phil. students and one Ph.D student guided. He is also member of Editorial Board of five journals in Research India Publications.

P. Lokesh Kumar Reddy, received the BCA and MCA degrees from S.V. University, Tirupati in 2004 and 2007. He is working as Assistant Professor in Rama Raja Institute of Technology and Science, Tirupati. His research interest Network Protocol.