JThB22.pdf

Design of Synchronous "Plug & Play" QKD-WDM-PON for Efficient Quantum Communications

Yi Zhao[1], Martin Roetteler, Lei Xu, and Ting Wang
NEC Laboratories America, 4 Independence Way, Princeton, NJ 08540, USA
Email: {mroetteler, leixu}@nec-labs.com

Abstract: We propose a new design of quantum key distribution (QKD) – WDM-PON with "plug & play" scheme and synchronization. Simulations show that the design can improve the quantum key generation rate 3 - 4 times over conventional schemes.
OCIS codes: (270.5565) Quantum communications; (060.4265) Networks, wavelength routing

1. Introduction

Quantum key distribution (QKD) [1] provides a means for secure communication between legitimate users. Its security is proven to be unconditional based on the fundamental laws of physics even if some components in the implementation are imperfect [2]. Despite of the commercialization of point-to-point QKD systems, the extension to applying QKD in network settings is of pivotal importance for its broad deployment, in particular using passive optical networks (PON). In a PON, all the components used between the central office (or optical line terminal, OLT) and the end network units (or optical network unit, ONU) are passive to minimize the network deployment cost. A PON also provides a platform for the implementation of QKD. The idea of implementing QKD in a time division multiplexing (TDM)-PON was first demonstrated in 1997 [3]. Using a "plug & play" structure [4], a QKD communication scheme on top of wavelength division multiplexing (WDM)-PON was further proposed [5]. Some of the challenges for the implementation of a QKD-PON include reducing the system cost and improving the quantum communication efficiency or quantum key generation rate per user. Compared with the QKD-TDM-PON scheme, a QKD-WDM-PON can achieve much higher quantum key generation rate per user. The "plug & play" QKD system structure can provide intrinsic stability against random polarization rotations during the optical signal transmission and the phase drift in the quantum transmitters [4].

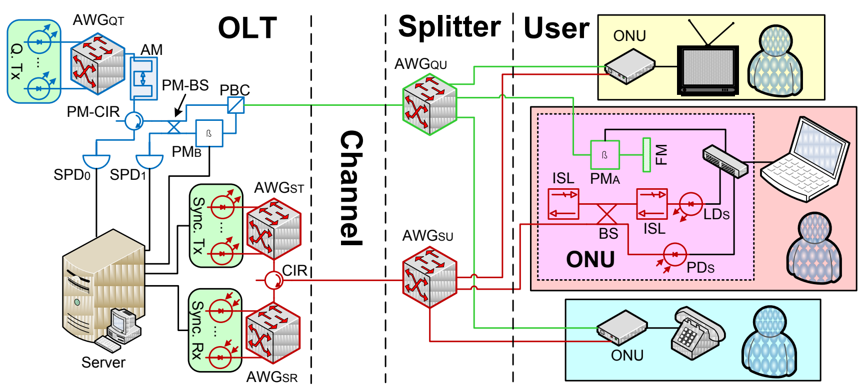


Fig. 1 Schematic of synchronous "plug & play" QKD-WDM-PON
LD: laser diode, CIR: circulator, BS: beam splitter, SPDx: single photon detector, PMx: phase modulator, PBC: polarization beam combiner, AWG: arrayed waveguide grating, FM: Faraday mirror, Q.Tx: quantum transmitter, AM: amplitude modulator, PM-BS: polarization maintaining beam splitter, PM-CIR: polarization maintaining circulator, Sync.Tx: synchronization transmitter, Sync.Rx: synchronization receiver, ISL: optical isolator, PD: photodiode. Blue line: polarization maintaining fiber, green line: quantum channel, red line: synchronization/classical channel.

2. System Design

Fig. 1 shows the schematic of our proposed synchronous QKD-WDM-PON using "plug & play" schemes. Note that two separate AWGs are adopted to avoid any possible crosstalk from the relatively high-power classical channels to the quantum channels. In the quantum communication part, one pair of single photon detectors (SPDs) are located at the OLT and shared by all the ONUs. With our proposed design, the quantum transmitters (Q. Tx) generate continuous wave light at different wavelengths, which are multiplexed with an AWG (AWG_{QT}) and are shaped into pulses at a repetition rate f_{rep} with an amplitude modulator (AM). For each quantum pulse generated, all the synchronization transmitters (Sync. Tx) send synchronization signals over the conventional WDM-PON

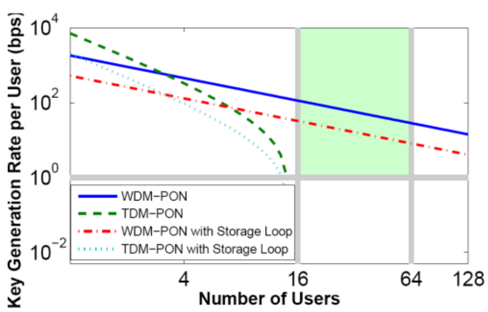
[1] Current address: California Institute of Technology, 1200 E California Blvd., MC 12-33, Pasadena, CA 91125, USA

channels. The photo diode at the ONU side (PD_S) detects the synchronization signal and triggers the user's phase modulator (PM_A) to encode the quantum information. The user then sends out a synchronization signal with the laser diode (LD_S) together with the returning quantum signal. At the OLT, the detection of the upstream synchronization signal triggers the phase modulator (PM_B) and the SPDs. If one of the SPDs clicks, the server records its bit value and its sender (i.e., which synchronization receiver (Sync. Rx) clicks).

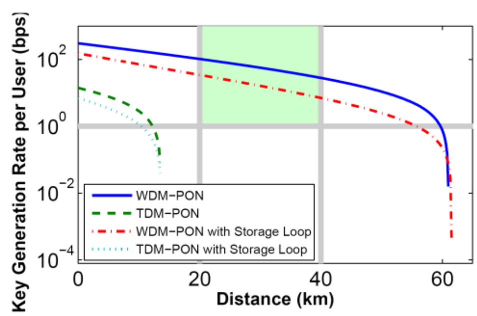
Compared with some previous QKD-WDM-PON designs [5], our proposal has several advantages. First, each user in the network can have both classical and quantum communications simultaneously as the synchronization channel can carry classical data stream together with the quantum synchronization signals. This is because the classical communication usually uses much higher repetition rate comparing to quantum communication. There are many "idle time" between adjacent quantum synchronization signals that can host classical data signals. Second, the down-stream quantum signals can be very weak since the synchronization is implemented separately. One can then substantially reduce the backscattering noise. Therefore, the ONU does not need an optical storage loop (OSL), which is costly and reduces the performance, but is required by most "plug & play" QKD systems without dedicated synchronization channels [4,5]. Finally, only one pair of single photon detectors (SPDs) are used in the PON system, and shared by all the users, significantly reducing the initial deployment and future upgrading costs. Note that, the number of SPDs that the OLT can use is flexible. The system performance can be improved by using more SPDs.

3. Numerical Simulation

We performed numerical simulations with the parameters from [6] to study the performance of our proposed system. Here we assume that the system adopts an ideal decoy state protocol [6,7]. Due to its "plug & play" nature, we adopt the security analysis for untrusted source QKD [7]. Fig. 2 (a) shows the simulation results on the impact of the number of PON users on the secure quantum key rate, with PON transmission distance to be 30 km. We can see that with a typical PON (having 16 to 64 users), our design (the blue solid line) yields a key rate well above 1 bit per second, which is often considered as the bottom line for "acceptable" quantum communication systems. As a comparison, the performance of the QKD-TDM-PON [3] deteriorates rapidly as the number of users increases. Moreover, a QKD-WDM-PON using an OSL [5] will decrease the key rate per user by about 70% within the typical PON usage, if compared with our synchronization design.



(a)



(b)

Fig. 2 (a) quantum key generation rate per user versus the number of users (PON transmission distance= 30 km) (b) quantum key generation rate per user v.s. the PON transmission distance (Number of PON users = 32). Green areas indicate parameters for typical PON usage.

Fig. 2(b) shows the correlation between the PON transmission distance and the secure key generation rate. Here we assume that the PON has 32 users. We can see that at typical PON distances (green area in Fig. 2(b)), the secure key generation rate of our design (the blue solid line) is well above 1 bit per second and substantially (3x-4x) greater than that of the QKD-TDM-PON scheme and a QKD-WDM-PON using an OSL within typical PON distance.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* pp. 175 – 179 (1984).
[2] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quant. Info. Compu 4, 325 (2004).
[3] P. Townsend, "Quantum cryptography on multiuser optical fiber networks," Nature 385, 47 (1997).
[4] A. Muller, T. Herzog, B. Hutter, W. Tittel, H. Zbinden, and N. Gisin, "'Plug & play' systems for quantum crytography," Appl. Phys. Lett. 70, 793 (1997).
[5] G. Brassard, F. Bussieres, N. Godbout, and S. Lacroix, "Multiuser quantum key distribution using wavelength division multiplexing," in *Proceedings of SPIE vol. 5260* p. 149 (2003).
[6] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental quantum key distribution with decoy states", Phys. Rev. Lett. 96, 070502 (2005)
[7] Y. Zhao, B. Qi, and H.-K. Lo, "Quantum key distribution with an unknown and untrusted source," Phys. Rev. A 77, 052 327 (2008).