# Multi–User Frequency–Time Coded Quantum Key Distribution Network Using a Plug-and-Play System

Y.T. Aladadi[1], A.F. Abas[1], Abdulmalik Alwarafy[1], M.T. Alresheedi[1]
[1]*Department of Electrical Engineering, College of Engineering, King Saud University, Riyadh 11421, Saudi Arabia*

yaladadi@ksu.edu.sa
aabas@ksu.edu.sa
437106913@student.ksu.edu.sa
malresheedi@ksu.edu.sa

*Abstract*— **In this paper, we propose and analyse a multi-user wavelength division multiplexing technique of frequency-time coded quantum key distribution that uses a plug and play scheme. Numerical simulation results show that the influence of the channel noise is reduced. At the same time, the final key rate per user is enhanced to be close to that of point-to-point link. This performance is the result of simultaneous communications between Alice and four Bobs.**

***Keywords*—Quantum Key Distribution, Plug-and-Play System, Wavelength Division Multiplexing, Frequency-Time Coding, Multi-Wavelength Laser Diode.**

## I. Introduction

Quantum Key Distribution (QKD) [1] is a good security solution for optical communication systems. It overcomes the imperfections of classical cryptography by providing a way to securely generate arbitrarily long cryptographic keys using the quantum properties of lights. In the reported literature, the implementations of QKD rely on the polarization coding [1, 2], phase coding [3, 4], frequency coding [5], time coding [6] and entanglement [7]. In case of a polarization coding, the information is carried by the state of polarization (SOP) that should be recovered at the receiver. This technique suffers from Polarization Mode Dispersion (PMD) and Polarization Dependent Loss (PDL)[3]. For the phase coding the quantum bit error rate (QBER) is related to the interference visibility, which is influenced by the noise of channel; therefore, feedback control is needed to stabilize the interferometer[8]. Differential phase coding schemes are introduced to compensate the drawbacks of phase coding schemes [9]. Disadvantages of QKD channels with frequency coding are associated, mainly, with strong levels of carrier and photon subcarriers in one optical fiber and its power grid [10].

A plug-and-play system is a round-trip two-way QKD system that can automatically compensate for the birefringence effect; therefore, it can operate stably for a long period of time without requiring any polarization control in a long optical fiber [4].

Frequency time coding scheme is introduced to reduce the influence of the channel noise [11]. Wavelength division multiplexing (WDM) QKD scheme has been introduced to overcome the inefficiency of splitter. Multi-user QKD systems that employs different wavelengths to transmit an optical pulses to multiple users have been introduced [12-15]. It is known in principle of communication that the final key rate per user decreased as 1/N, where N is the total number of subscribers.

In this paper, we propose and analyses a multi-user wavelength division multiplexing of frequency-time coded (FT) QKD that uses a plug-and-play scheme. QKD based frequency and time coding has lower QBER as compared to other techniques [11]. Combining the plug and play system with WDM maintains the key rate per user to values that are close to that in case point-to-point communication [16].

## II. Point-to-Point Frequency-time Coded QKD scheme

In frequency time coded QKD (FT-QKD) [11], the key is encoded in the frequency and time between Alice and Bob. The proposed point-to-point FT-QKD scheme is shown in Fig. 1. There are two laser diodes, LD1 and LD2, which operate at different designed wavelengths. Both lasers are employed for frequency coding.

For the third laser diode (LD3), time delay is introduced for realizing time coding. LD1 and LD2 generate narrow pulses (in frequency domain) with central wavelengths $\lambda_1$ and $\lambda_2$, respectively as shown in Fig. 2; whereas $\lambda_3$ is considered as central frequency of LD3. The bandwidth of the pulse generated by LD3 should be at least the double of that in LD1 or LD3 because the detection gate duration is twice of the width of the pulse sent [11].

978-3-903176-07-2 © 2018 IFIP

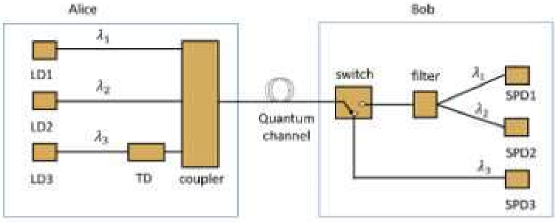

Fig. 1 Schematic of point to point (PTP) FT-QKD system

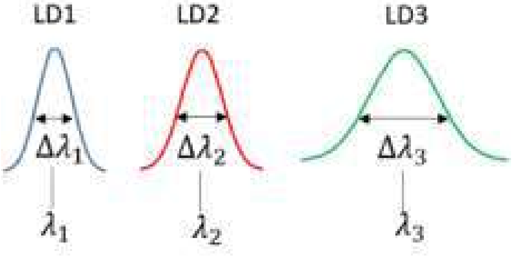

Fig. 2 The frequency domain of laser diodes pulses

To understand how this system works, let us consider that Alice and Bob generate 11 qubits with 11 basis randomly as described in Table I.

**Table I: The Bits and Basis Generated By Alice and Bob**

| | |
|---|---|
| Alice's bits: | 10000101011 |
| Alice's basis: | 00100110000 |
| Bob's bits: | 10111010101 |
| Bob's basis: | 00110101100 |

The transmitted photons according to both bits and basis of Alice are shown in Fig. 3. It is clear that when the basis is zero, the frequency coding is selected; whereas time coding is selected when the basis is one.

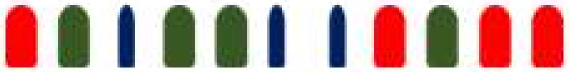

Fig. 3 The transmitted photons

In case of frequency coding, and the bit is zero, the LD1 is fired; whereas LD2 is fired when the transmitted bit is one. In other hand, the time delay is zero when bit is zero and the LD3 is the selected laser according to the basis. When the selected bit is one and LD3 is fired, the time delay (TD) is adjusted to τ.

The transmitted photons are combined at coupler to be transmitted through a quantum channel (QC). The optical switch at Bob works according to Bob's basis. This mean that optical switch operates according to Bob's basis. The received phonons are detected by three single photon detectors that operate at different designated wavelengths. The photons after detection process are shown in fig. 4. It is clear that the received photons by detectors are these with the same basis at both Alice and Bob.

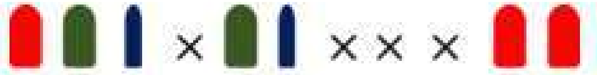

Fig. 4 The received photons

## III. System Setup

Fig. 5 shows the proposed system setup. Instead of using single laser diode, multi-wavelength laser diode (MW-LD) is employed. Wavelength selective switch (WSS) is used to select the four pulse signals with differently designated wavelengths generated by MW-LD. As mentioned in Section II, MW-LD1 and MW-LD2 are used in the case of frequency coding; whereas MW-LD3 and TD are employed for time coding. The pulses from three multi-laser are combined using a multiplexer and passed through a circulator (CIR), and subsequently launched into the quantum channel (QC). The variable attenuator (VA) at each Bob is set to a low level and bright laser pulses are emitted by Alice [17]. The transmitted photons pass through two quantum channels, and this makes the distance between Alice and the other four users different. So, time delay and line delay are required to tune the arrival time of the returned pulses in a group to be the same. This helps to reduce the impact of Rayleigh backscattered light [16]. On the other hand, a waiting time will reduce the final key rate.

To understand the principle of the proposed system, let Alice and four Bob generate their bits and basis randomly as shown in Table II.

Table II: The Bits Generated By Alice and the Four Bobs

| | |
|---|---|
| Alice's bits: | 10000101011 |
| Alice's basis: | 00100110000 |
| Bob1's bits: | 10111010101 |
| Bob1's basis: | 00110101100 |
| Bob2's bits: | 10111111101 |
| Bob2's basis: | 00100101101 |
| Bob3's bits: | 10111111101 |
| Bob3's basis: | 11001011101 |
| Bob4's bits: | 11100000001 |
| Bob4's basis: | 10100010100 |

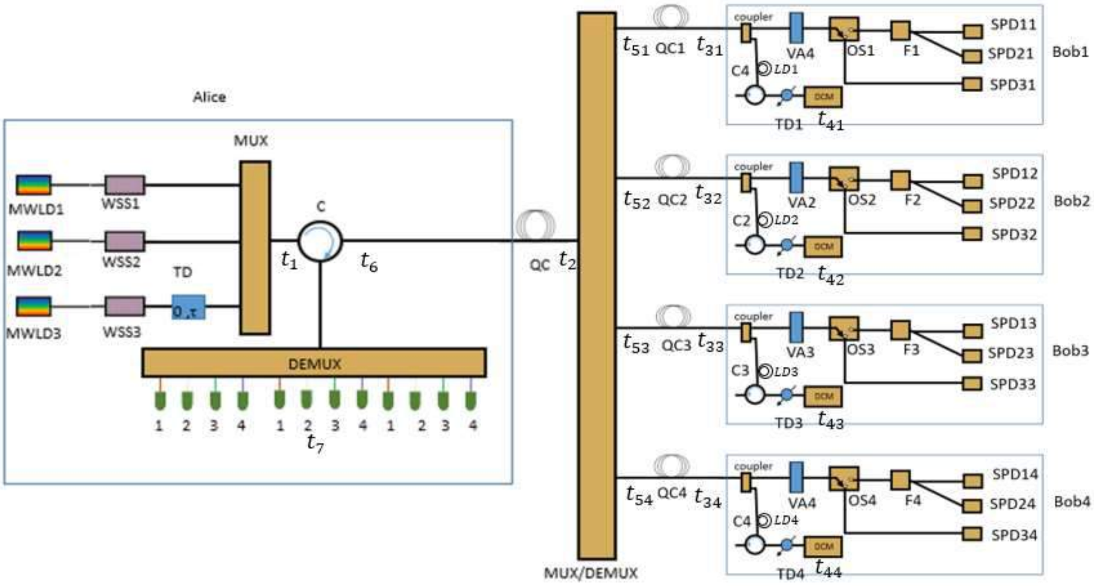

Fig. 1 Schematic of multi-user WDM-FT QKD system

Fig.6 shows the process of pulse transmission at seven positions $t_1$, $t_2$,…, and $t_7$. Time position $t_1$ refers to the pulse group after the multiplexer. Then, the pulse group is passed through the QC, before entering the MUX/DEMUX as marked at $t_2$. At $t_3$, due to the possibility that QC of each user has different length, Bob $i$ may receive the transmitted photons before Bob $j$ and each one receives the transmitted photons according to his's basis. At $t_4$, the four users complete the reception process, and the driver and control module collects the data and reflects it to Alice with different delay [11]. Therefore, a time delay and line delay are needed to compensate this

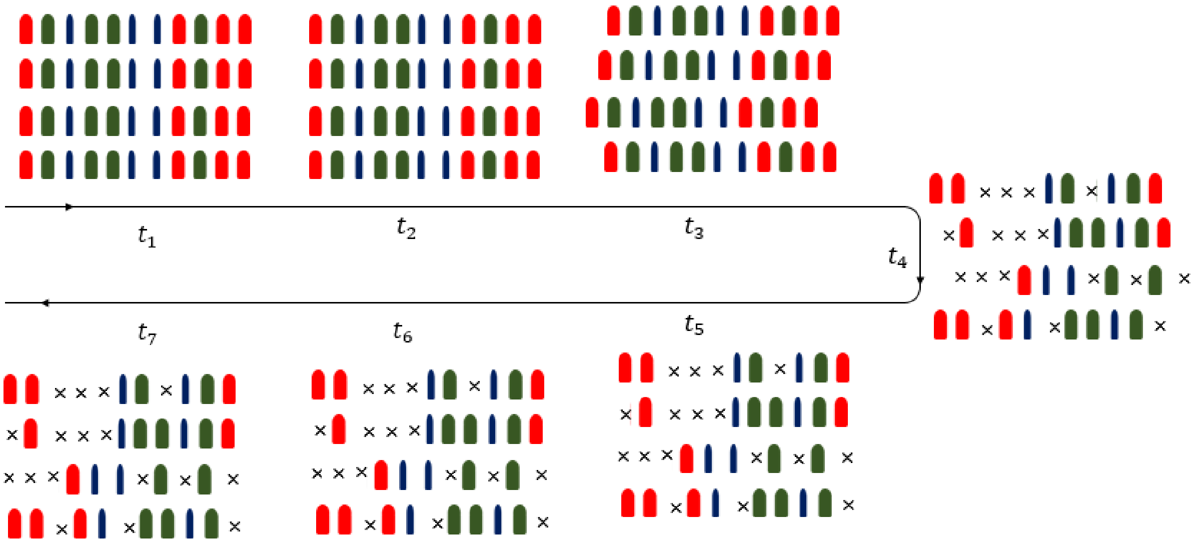

Fig. 2 The pulse transmission process, starting from $t_1$ to $t_7$

shortage. It is clear that at $t_5$, the received photons by all users have the same positions. At $t_7$, Alice compares her basis with the basis of each user. Then she calculates QBER. If QBER < QBER$_{thr}$ , then eavesdropper (Eve) exits, QKD falses and retransmits the photons. Otherwise, if QBER > QBER$_{thr}$, Alice and each user (Bob *i*) obtain the final key that has the same basis after data reconciliation and privacy amplification. According to comparison, the final key rates of Alice and the four Bobs are given in Table III.

Table III: **The Final Key Rates of Alice and the Four Bobs**

| | |
|---|---|
| 7 basis matches. | |
| Alice's key: | 1000111 |
| Bob1's key: | 1011001 |
| 7 basis matches. | |
| Alice's key: | 1000011 |
| Bob2's key: | 1011110 |
| 5 basis matches. | |
| Alice's key: | 00101 |
| Bob3's key: | 01111 |
| 8 basis matches. | |
| Alice's key: | 00000111 |
| Bob4's key: | 11000001 |

## IV. Results and Discussion

The sifted key rate and quantum bit error rate (QBER) are the most important parameters used to evaluate a QKD system. The sifted key rate (Raw rate) [17] is given by:

$$R_{raw} = \frac{1}{2} f_r \, \mu t_{AB} t_B \eta_B \tag{1}$$

where $\mu$ denotes the mean photon number of each weak coherent pulse, $f_r$ is the pulse repetition rate, $t_{AB}$ is the transmittance of the link from Alice to Bob, $t_B$ is Alice's internal transmittance and $\eta_B$ is Alice's detector efficiency. $R_{raw}$ is the same for both BB84 protocol (the first implementation method of QKD that uses phase coding or polarization coding) and for FT coding [11, 17, 18]. The difference appears in the QBER, in which QBER of BB84 protocol is given by [16]:

$$QBER_{BB84} = \frac{1-V}{2} + \frac{p_{dark}}{\mu t_{AB} t_B \eta_B} + \sum_{n=0}^{\frac{1}{p_{det}}} p_{after}\left(\tau + n\frac{1}{f_r}\right) \tag{2}$$

where V denotes the visibility of the interference meter, p$_{dark}$ is the probability of a dark count per gate, p$_{det}$ is the probability of a detector click, p$_{after}$ is the probability of an after-pulse over all and τ is the detector's dead time. Both $p_{dark}$ and $p_{after}$ depend on the characteristics of the photon counters. For FT protocol, suppose that the operating wavelength is 1550 nm, and $\Delta t_1$ ($\Delta t_2$) be 1000 ps, and $\Delta t_3$ is 500 ps, and the associated $\Delta\lambda_1$ ( $\Delta\lambda_2$ ) is $8 \times 10^{-3}\, nm$ , and $\Delta\lambda_3$ is $16 \times 10^{-3}\, nm$. The detection gate duration is double that of sent pulse duration. Therefore, the effect of time spread and frequency spread from dispersion on detection results can be neglected [11]. So, the first part of Eq. 2 is set to zero when the basis is the same. The QBER of FT protocol is given as:

$$QBER_{FT} = \frac{p_{dark}}{\mu t_{AB} t_B \eta_B} + \sum_{n=0}^{\frac{1}{p_{det}}} p_{after}\left(\tau + n\frac{1}{f_r}\right) \tag{3}$$

In our proposed scheme, a time delay and line delay are taken into account. Therefore, raw kay rate is derived as:

$$\hat{R}_{raw} = \frac{\frac{1}{2} f_r \, \mu t_{AB} t_B \eta_B t_{ex} + \frac{1}{2} f_r \, \mu t_{BA} t_A \eta_A \, \eta_{TD} t_{ex}}{2} \tag{4}$$

and,

$$t_{AB} = 10^{-\frac{\alpha L}{10}} \tag{5}$$

$$t_{BA} = 10^{-\alpha(L+L_{LD})/10} = t_{AB} 10^{-\frac{\alpha L_{LD}}{10}} \tag{6}$$

$$\eta_{TD} = \frac{1}{1 + t_{TD}} \tag{7}$$

where, $L$ is the fiber length between Alice and Bob, LLD is the fiber length of line delay, $t_{TD}$ is time delay at Bob, and $t_{ex}$ is the extra transmittance due to MUX and DEMUX.

Let , $t_B = t_A$ , $\eta_B = \eta_A$. So, raw key rate can be described as:

$$\bar{R}_{raw} = \frac{\frac{1}{2} f_r \, \mu t_{AB} t_B \eta_B t_{ex} \left(1 + \ 10^{-\frac{\alpha L_{LD}}{10}} \eta_{TD}\right)}{2} \tag{8}$$

$$\bar{R}_{raw} = \frac{1}{4} f_r \, \mu t_{AB} t_B \eta_B t_{ex} \left(1 + \ 10^{-\frac{\alpha L_{LD}}{10}} \eta_{TD}\right) \tag{9}$$

QBER due to the dark count probability is modified as shown in Eq. 10.

$$\overline{QBER} = \frac{p_{dark}}{2\mu t_{AB} t_B \eta_B t_{ex}} + \frac{1}{2} \sum_{n=0}^{\frac{1}{p_{det}}} p_{after}\left(\tau + n\frac{1}{f_r}\right) + QBER_{BA} \tag{10}$$

$$QBER_{BA} = \frac{p_{dark}}{2\mu t_{BA} t_A \eta_A \eta_{TD} t_{ex}} + \frac{1}{2} \sum_{n=0}^{\frac{1}{p_{det}}} p_{after}\left(\tau + n\frac{1}{f_r}\right) \tag{11}$$

$$\overline{QBER} = \frac{p_{dark}}{2\mu t_{AB} t_B \eta_B t_{ex}}\left(1 + \frac{10^{\frac{\alpha L_{LD}}{10}}}{\eta_{TD}}\right) + \sum_{n=0}^{\frac{1}{p_{det}}} p_{after}\left(\tau + n\frac{1}{f_r}\right) \quad (12)$$

Final key rate of the proposed scheme is given by:

$$\bar{R}_{final} = \frac{1}{4} f_r\, \mu t_{AB} t_B \eta_B t_{ex}(I_{AB} - I_{AE}) + \frac{1}{4} f_r\, \mu t_{BA} t_A \eta_A\, \eta_{TD}(I_{BA} - I_{BE}) t_{ex} \quad (13)$$

$$I_{AB} = 1 - H_2(QBER_{FT}) \quad (14)$$

$$I_{BA} = 1 - H_2(QBER_{BA}) \quad (15)$$

$$I_{AE} = \mu(1 - t_{AB}) + 1 - V \quad (16)$$

$$I_{AE} = \mu(1 - t_{BA}) + 1 - V \quad (17)$$

where $I_{AE}$ denotes the mutual information between Alice and Eve, and $H_2(Q)$ is the binary entropy which is defined as [19]:

$$H_2(Q) = -Qlog_2(Q) - (1 - Q)log_2(1 - Q) \quad (18)$$

The parameters used in the numerical simulation are summarized in Table IV.

**Table IV: Simulation Parameters.**

| Parameter | Value |
|---|---|
| Pulse repetition rate ( $f_r$) | 4MHz |
| Pulse width | 500 ps, 1000 ps |
| Average number of photons per pulse (μ) | 0.1 |
| Transmittance of MUX and DEMUX | 0.9 |
| Fiber attenuation coefficient (α) | 0.2 dB/km |
| Detector efficiency at 1,550 nm ($\eta_A$) | 10% |
| Probability of dark count ($p_{dark}$ ) | 10−5/gate |
| Probability of a detector click ($p_{det}$ ) | 0.15% |
| Detection gate | 2 ns |
| Dead time (τ) | 10 µs |
| Fringe visibility (V) | 0.8 , 0.9 |
| Transmittance of Bob's system ($t_B$) | 0.6 |
| After-pulse count probability ($p_{after}$ ) | 4% |
| Bob' delay line (LDL) | 10 km |

Fig. 7 shows the QBER of three case, BB84 point-to-point (PTP), FT PTP, and multi user FT system, for different fringe visibility (V). From this figure, it is clear that BB84 protocol is sensitive to V, where decreasing V, gives wore QBER. For example, at L =100 km, QBER is about 0.237 at V=0.9, and 0.287 at V=0.8. The results in Fig. 7 show that independent on the value of V, FT reduces the QBER to 0.187 compared to BB84. The line delay in FT MU system is about 10 km, and this causes a small increase in QBER, 0.24, compared to FT PTP, 0.187. However, FT still better than BB84 for fiber length L< 100 km.

Fig. 8 shows the final key rate against fiber length. Final key rate is very sensitive to V. For instance, at L = 10 km, changing V from 0.9 to 0.8, decreases the final key rate from 4204 b/s, 5601 b/s, and 6182 b/s to 2105 b/s, 4919 b/s and 5425 b/s for BB84 PTP, FT PTP, and FT MU systems, respectively. However, the amount of change in FT system is very small and still work in worse visibility compared with BB84 system. Furthermore, it is clear that the key rate per user in FT MU maintains a high level compared with FT PTP because the communications between Alice and four Bobs can be carried out simultaneously. Meanwhile, when $V = 0.9$ , and $\bar{R}_{final}$=3000 b/s, the communication distance of FT PTP and FT MU are increased by 9 Km, and 7 km respectively compared to BB84 system. Also, it is clear that the proposed Multi user-QKD network provides a better performance in situations in which all users share a similar quantum channel.

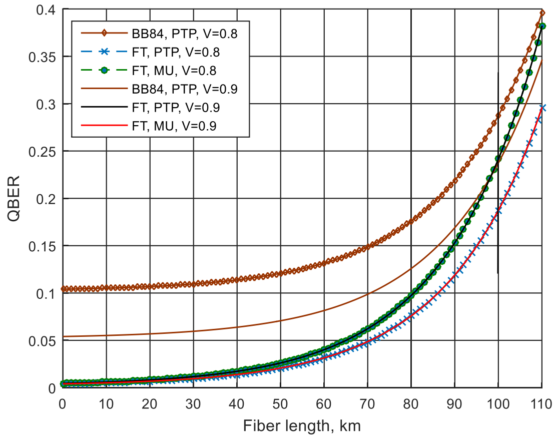

Fig. 7 The QBER versus fiber length between Alice and Bob, for three case, BB84 PTP, frequency time coding PTP, and frequency time coding MU, V=0.8, 0.9, $L_{LD}$=10 km

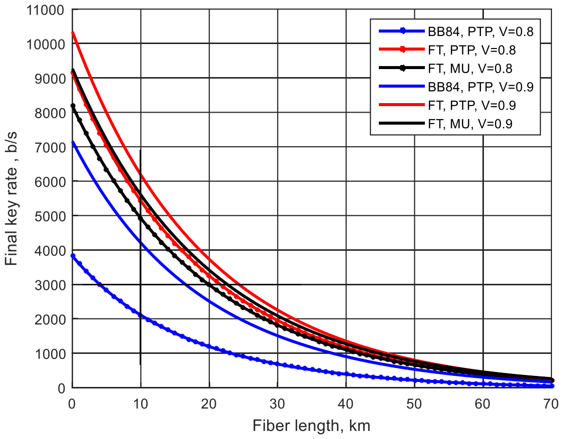

Fig. 8 The final key rate versus fiber length between Alice and Bob, for three case, BB84 PTP, frequency time coding PTP, and frequency time coding MU, V=0.8, 0.9, $L_{LD}$=10 km

## Acknowledgment

The project was supported by King Saud University, Deanship of Scientific Research, College of Engineering Research Center.

## V. Conclusion

Frequency and time coding reduce the QBER as compared to BB84 that employs polarization coding or phase coding. Our simulation results show that the FT protocol can work at worse visibility, and offers extra distance. Furthermore, a multi-user WDM-QKD uses the same principle of FT scheme, where QBER is still less than that of BB84 protocol. Meanwhile, the key rate per user maintains a high level compared to point-to-point links. This is because the communications between Alice and four Bobs can be carried out simultaneously.

## References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical computer science,* vol. 560, pp. 7-11, 2014.

[2] N. Namekata, G. Fujii, S. Inoue, T. Honjo, and H. Takesue, "Differential phase shift quantum key distribution using single-photon detectors based on a sinusoidally gated In Ga As / In P avalanche photodiode," *Applied physics letters,* vol. 91, p. 011112, 2007.

[3] H. Zbinden, N. Gisin, B. Huttner, A. Muller, and W. Tittel, "Practical aspects of quantum cryptographic key distribution," *Journal of Cryptology,* vol. 13, pp. 207-220, 2000.

[4] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "“Plug and play” systems for quantum cryptography," *Applied physics letters,* vol. 70, pp. 793-795, 1997.

[5] J.-M. Merolla, Y. Mazurenko, J.-P. Goedgebuer, and W. T. Rhodes, "Single-photon interference in sidebands of phase-modulated light for quantum cryptography," *Physical review letters,* vol. 82, p. 1656, 1999.

[6] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, and F. Vannel, "Continuous high speed coherent one-way quantum key distribution," *Optics express,* vol. 17, pp. 13326-13334, 2009.

[7] F. Xu, B. Qi, Z. Liao, and H.-K. Lo, "Long distance measurement-device-independent quantum key distribution with entangled photon sources," *Applied physics letters,* vol. 103, p. 061101, 2013.

[8] Z. Yuan and A. Shields, "Continuous operation of a one-way quantum key distribution system over installed telecom fibre," *Optics express,* vol. 13, pp. 660-665, 2005.

[9] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Physical review letters,* vol. 89, p. 037902, 2002.

[10] I. M. Gabdulhakov and O. G. Morozov, "Frequency coded quantum key distribution channel based on photon amplitude-phase modulation," in *Systems of Signal Synchronization, Generating and Processing in Telecommunications (SINKHROINFO), 2017*, 2017, pp. 1-5.

[11] Z. Chang-Hua, P. Chang-Xing, Q. Dong-Xiao, G. Jing-Liang, C. Nan, and Y. Yun-Hui, "A new quantum key distribution scheme based on frequency and time coding," *Chinese Physics Letters,* vol. 27, p. 090301, 2010.

[12] J. Bogdanski, N. Rafiei, and M. Bourennane, "Multiuser quantum key distribution over telecom fiber networks," *Optics Communications,* vol. 282, pp. 258-262, 2009.

[13] P. D. Kumavor, A. C. Beal, E. Donkor, and B. C. Wang, "Experimental multiuser quantum key distribution network using a wavelength-addressed bus architecture," *Journal of lightwave technology,* vol. 24, p. 3103, 2006.

[14] C. Autebert, J. Trapateau, A. Orieux, A. Lemaître, C. Gomez-Carbonell, E. Diamanti, I. Zaquine, and S. Ducci, "Multi-user quantum key distribution with entangled photons from an AlGaAs chip," *Quantum Science and Technology,* vol. 1, p. 01LT02, 2016.

[15] V. Fernandez, K. J. Gordon, R. J. Collins, P. D. Townsend, S. D. Cova, I. Rech, and G. S. Buller, "Quantum key distribution in a multi-user network at gigahertz clock rates," in *Photonic Materials, Devices, and Applications*, 2005, pp. 720-728.

[16] G. Cheng, B. Guo, C. Zhang, J. Guo, and R. Fan, "Wavelength division multiplexing quantum key distribution network using a modified plug-and-play system," *Optical and Quantum Electronics,* vol. 47, pp. 1809-1817, 2015.

[17] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," *New Journal of Physics,* vol. 4, p. 41, 2002.

[18] B. Qi, "Quantum key distribution based on frequency-time coding: security and feasibility," *arXiv preprint arXiv:1101.5995,* 2011.

[19] C. Macchiavello, G. M. Palma, and A. Zeilinger, *Quantum Computation and Quantum Information Theory: Reprint Volume with Introductory Notes for ISI TMR Network School, 12-23 July 1999, Villa Gualino, Torino, Italy*: World Scientific, 2000.