PERFORMANCE ANALYSIS OF CV-QKD USING MULTICORE FIBER

Thu A. Pham*

* Faculty of Telecommunications, Posts and Telecommunications Institute of Technology, Hanoi, Vietnam

Abstract: In this paper, we have proposed a quantum key distribution (QKD) system employing multi-core fiber (MCF). We then theoretically analyze the system performance comprehensively while considering various physical impairments including noise and MCF crosstalk. The feasibility of the proposed architecture is verified via the numerical experiments. The simulation results demonstrate that our developed solution can significantly enhance the secret key rate. It is also shown that the system performance strongly depends on the kind of MCFs.

Keywords: Quantum Key Distribution (QKD), Multi-core fiber (MCF).

I. INTRODUCTION

In the digital era in which data traffic has been continuously experiencing an exponential rise across the globe, the enormous data which is called plain text is being liable to a lot of great security threats. The security of data interaction between the network systems depends on the adopted security protection mechanism. Although there are many information encryption mechanisms used for different systems, the commonality is that the security of the key directly affects the safe operation of the network systems.

As a new method to ensure the secure transmission of information, quantum key distribution (QKD) technology which provides an unconditionally secure method of sharing secret keys between the legal pair of sender and receiver, Alice and Bob, in the presence of an illegal eavesdropper known as Eve has attracted the attention of many researchers and deployers and has successively carried out verification tests in many fields. The secrecy of the keys distributed by QKD is based on the laws of quantum mechanics and could be implimented by using the polarization or phase of single-photon states, namely discrete-variable QKD (DV-QKD), or using the quadrature of the quantized electromagnetic field, namely continuous variable QKD (CV-QKD). DV-QKD schemes could be employed to deliver the unconditionally secure keys between two legal nodes. However, the approaches have some limitations such as limited achievable transmission distance and low secret key rate. Moreover, the technologies used in DV-QKD system are quite different from the technologies used in conventional communications. To cope with these disavantages, CV-QKD scheme which have potential advantages because of its capability of obtaining high secure key rate has been of interest. In addition, compared to DV-QKD, CV-QKD can make use of traditional telecommunication technologies.

Recently, CV-QKD systems have been suggested and several multiplexing technologies, for example WDM, polarized or phase mutiplexing, have been established to enhance the performance of these systems [1-3]. However, the multiplexing technologies require sophiticated devices rather than commercial devices and the secret key rates of the CV-QKD systems are still far from the demands of the practical implementation. In the last few years, spacial division multiplexing (SDM) technology, which uses the multillicity of space channels to rise capacity, has been proposed to keep up with the emmense trafic demand [4-6]. One actualizing approach of SDM transmission media is multicore fiber (MCF) which include many cores exploited as parallel channels for independent signals. MCF can be fully utilized as a transmission media to increase the capacity of QKD systems, and to break through the bottleneck of the secret key rate in the conventional SMF-based system [7-9].

Until now, some experimental works related to the use of MCF for CV-QKD scheme have been reported. In [10], the operation of co-transmission of CV-QKD and classical data channels over the same MCF has been successfully demonstrated. The works showed the slight degradation in performance of these systems. However, the method to increase secret key rate was not mentioned in these cases. A more recent work have model the CV-QKD transmition over MCF [11]. In this report, researchers proposed the MCF based CV-QKD system to further increase the secret key rate. The results in [12] showed that there was a negligible degradation in performance because of insert loss of the FIFO. Furthermore, the total secret key rate could be improved apparently. However, in this case, the distribution of quantum channel wavelength in each core is different and therefore the impact of MCF crosstalk could not be investigated.

In this paper, we propose to implement CV-QKD system over MCF. Our proposed MCF-based CV-QKD system could be a good solution to increase the secret key rate by transmitting multiple spatial modes simultaneously. Performance of the proposed MCF based CV-QKD system is analyzed in terms of quantum bit

Contact author: Thu Anh Pham
Email: thupa@ptit.edu.vn
Received: 6/5/2021, revised: 01/7/2021, accepted: 13/7/2021

error rate (QBER) considering the effects of various physical layer impairments originated from the receiver, and the impact of inter-core crosstalk in MCF channel. Moreover, ergodic secret key rate in the present of eavesdropper (i.e., Eve) is also the subject of this paper.

The rest of this paper is arranged as follows. Section II shows the CV-QKD architecture using MCF. Mathematical model and performance analysis are provided in Section III. The numerical results of the proposed system are presented and discussed in section IV. Finally, Section V closes the paper with some relevant conclusions.

II. SYSTEM ARCHITECTURE

Figure 1 schematically depicts our proposed CV-QKD system using MCF as the transmission media. The proposed system has three main parts, including a key sender (i.e. Alice's side), a key relayer where Eve could take the key, and Bob's side which receives the key signal to recover the quantum keys transmitted from Alice. QKD protocol implemented in this study is based on SIM using binary phase shift keying (SIM-BPSK).

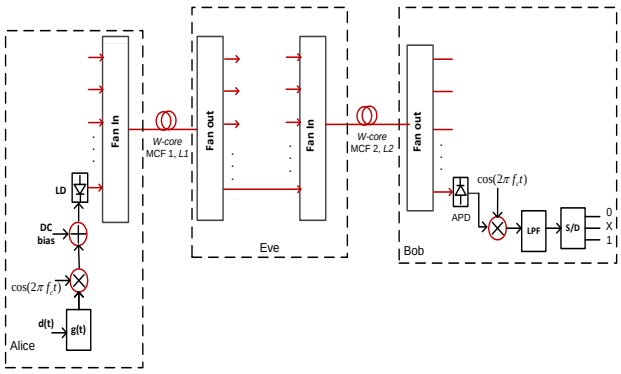


Figure. 1. The architecture of CV-QKD system using MCF

As shown in Fig. 1, at the Alice's side, the key's binary bits, $d(t)$, are passed to the rectangular pulse shaping function and modulated on RF subcarrier using BPSK signaling, in which bits "0" and "1" are represented by two phases that are 180^0 apart. Next, the BPSK signal, which includes both positive and negative values, is added to a DC bias before modulating with the optical continuous-wave generated by a laser diode (LD).

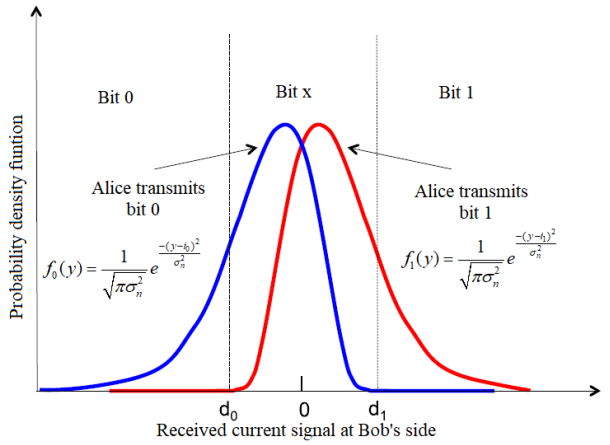


Figure 2: Dual-threshold detection at Bob's side [13]

The modulated optical signal from each LD is coupled into a specific core of the W-cores of MCF with the length of L_1 by using a fan-in device, and then transmitted via the MCF to relayer, where a fan-out device is used to demultiplex the optical signals and then a fan-in device is employed to multiplex the modulated optical signals. The signal after fan-in device is transmitted via another W-core MCF with the length of L_2 to the Bob's side.

At the Bob's side, the received optical signal demultiplexed from the MCF is passed through an APD to convert into an electrical signal. Then, the electrical signal is demodulated by multiplying with local oscillator's signal, whose frequency is equal to that of RF subcarrier (f_c). After demodulating process, the electrical signal is sampled and decided to binary bits "0", "1", or "x" based on dual-threshold (D-T) detection. As can be seen from the Figure 2, two levels of dual-threshold, d_0 and d_1, are set at Bob's receiver for signal detection. If the received current signal is lower than d_0, bit "0" will be recovered. If the received signal is larger than d_1, bit "1" will be detected. Otherwise, bit "x" (no bit) will be created. Probability density functions when bit 0 ($f_0(y)$) is transmitted and bit 1 ($f_1(y)$) is transmitted are shown in figure 2.

Finally, Bob notifies Alice the time instances when bits "0" and "1" were created via classical public channel. Based on the information shared by Bob, Alice could form the sifted key by removing bits corresponding to the time instances Bob created no bit.

III. PERFORMANCE ANALYSIS

In this section, the performance of the proposed system in terms of quantum bit error rate and secret key rate will be evaluated.

As can be seen from figure 1, at the Alice's transmitter, the binary bits of key, $d(t)$, are passed to the rectangular pulse shaping function and modulated on RF subcarrier using BPSK signaling, in which bits "0" and "1" are represented by two phases that are 180^0 apart. Next, the BPSK signal, which includes both positive and negative values, is added to a DC bias before modulating with the optical continuous-wave generated by a laser diode (LD). It is noted that the LD can only be modulated by the positive signals. The transmitted power of the modulated laser beam could be written as follows

$$P_t(t)=\frac{P_o}{2}\left[1+mS(t)\right], \quad (1)$$

where P_o is the peak transmitted power, m is the intensity modulation depth with $0 < m < 1$. $S_t(t) = A(t)g(t)\cos(2\pi f_c t + a_i\pi)$, where $A(i)$ is the carrier amplitude, $g(t)$ is the rectangular pulse shaping function, f_c is the carrier frequency, and $a_i \in \{0,1\}$ is the i th binary bit. The power of $S(t)$ is normalized to unity to simplify our analysis.

The modulated optical signal after each LD is coupled into a specific core (in the total of the w cores of the MCF 1) by using a low loss and low crosstalk fan-in device. The optical signals are then transmitted via the w-core MCF 1 with the length of L_1 to relay node, where a fan-out device is used to couple out the multiplexed optical

signals. After that, the modulated optical signals including the signal from Alice sent to Bob is again coupled into a *w*-core MCF 2 with the length of L_2 by using aother fan-in devicce. At the relay node, Eve can take and decode the information.

At the Bob's side, there is a fan-out device used to couple out the multiplexed optical signals. The received optical signal from Alice's side is passed through an optical band pass filter (OBPF) to reduce background noise. After that, the filtered signal is converted into an electrical one by APD. The electric current after APD can be expressed as

$$i_p(t) = \Re M_A \frac{P_{orB}}{2}\left[1 + mS(t)\right] + n_{rB}(t), \quad (2)$$

where $\Re$ and M_A are the responsivity and the gain of APD, respectively. n_{rB} is the receiver's noise current at the receiver of Bob. P_{orB} is the peak received power at Bob's side. This parameter is calculated as

$$P_{orB} = P_o.\exp\left[\alpha\left(L_1 + L_2\right)\right], \quad (3)$$

where α is the attenuation coefficient of the fiber and L_1 and L_2 are the optical fiber lengths of MCF 1 and MCF 2, respectively.

Then, the electric signal after APD is demodulated by multiplying with local oscillator's signal, whose frequency is equal to that of RF subcarrier. The BPSK demodulated precess is carried out by multiplexing the received signal with $\cos(2\pi f_c t)$. The current obtained after demodulation can be passed to a low-pass filter (LPF) to remove the high-frequency components (i.e., f_c and $2f_c$), the baseband signal obtained from the output of the LPF is given as

$$r(t) = \begin{cases} i_0 = -\frac{1}{4}\Re M_A P_{orB} m + n_{rB}(t) \\ i_1 = +\frac{1}{4}\Re M_A P_{orB} m + n_{rB}(t) \end{cases}, \quad (4)$$

where i_0 and i_1 represent the received signals for bits "0" and "1", respectively. The total noise variance is computed as folows.

When transmitting over the MCF, the optical signal on each core suffers from inter-core crosstalk (XT) caused by adjacent cores. For simplicity, we assume MCF is homogeneous (i.e., all cores have the same size and the refractive index). Considering a given core (i.e., the core *i*), the crosstalk between two cores is the ratio of the output power of the core *i* originating from an interfering core (i.e., core *j*) to that of the interfering core [14]. Therefore, the inter-core crosstalk between the two cores *i* and *j* in MCF is defined as [15]

$$XT_{ij} = \frac{P_{ij}}{P_j}, \quad (5)$$

where P_{ij} is the power in the core *i* coupling from core *j*, and P_j is the power in the core *j*.

On the other hand, in multi-core fiber, the coupled power is determined by the amount of the power that the signal being transmitted in one core is transferring to its adjacent core. The average mode coupling coefficient (K_{ij}) between two cores can be calculated, when the mode coupling coefficient from core *j* to core *i* is known, as [16]

$$K_{ij} = \kappa_{ij} - C_{ij}\frac{\Delta\beta_{ij}}{2}, \quad (6)$$

where κ_{ij} is the usual mode coupling coefficient from core *j* to core *i*, $\Delta\beta_{ij} = \beta_i - \beta_j$ is the propagation constant difference with β_i and β_j being mode propagation constants in core *i* and core *j*, respectively. Here, C_{ij} is the cross-power.

Moreover, the expression of the coupled power can be established as [17]

$$\frac{dP_i}{dz} = \sum_{j \neq i} h_{ij}(z)\left[P_j(z) - P_i(z)\right], \quad (7)$$

where P_i is the average power in the core *i* and h_{ij} is the power coupling coefficient from the core *j* to the core *i*. In case of the homogeneous MCF, the average power coupling coefficient between two adjacent cores *i* and *j* is calculated as [15,18]

$$\overline{h_{ij}} = \sqrt{2}K_{ij}^2 d\left[\frac{1}{\sqrt{a(b+\sqrt{ac})}} + \frac{1}{\sqrt{c(b+\sqrt{ac})}}\right], \quad (8)$$

with

$$a = c = 1 + \left(\frac{B_{ij}d}{R_{bd}}\right)^2, \quad (9)$$

$$b = 1 - \left(\frac{B_{ij}d}{R_{bd}}\right)^2, \quad (10)$$

$$B_{ij} = \sqrt{\left(\beta_i x_i - \beta_j x_j\right)^2 + \left(\beta_i y_i - \beta_j j_j\right)^2}, \quad (11)$$

where *d* is the correlation length, R_{bd} is the bending radius, β is the propagation constant while $\{x_i, y_i\}$ and $\{x_j, y_j\}$ are the positions of the *i*-th core and the *j*-th core, respectively.

Note that, in the homogeneous MCF, it can be considered that $\beta_i = \beta_j = \beta$, thus, we have $K_{ij} = \kappa_{ij} = \kappa$ and $B_{ij} = \beta\Lambda_{ij}$, where Λ_{ij} is the core pitch (i.e., the distance that separates core *i* and core *j*). Hence, the average of h_{ij} can be calculated for the case of small bending radius as

$$\overline{h_{ij}} = \frac{2\kappa^2 R_{bd}}{\beta\Lambda_{ij}}, \quad (12)$$

where R_{bd} is the bending radius.

Furthermore, the crosstalk between two adjacent cores can be computed as given in [21],

$$XT_{ij} = \tanh(\overline{h_{ij}}L) \approx \overline{h_{ij}}L \quad XT_{ij} = \tanh\left(\overline{h_{ij}}L\right) \approx \overline{h_{ij}}L, \quad (13)$$

where $L = L_1 + L_2$ is the total MCF length. Therefore, based on (12) and (13), the crosstalk can be expressed as

$$XT_{ij} = \frac{2\kappa^2 R_{bd}}{\beta \Lambda_{ij}} L \text{ , (14)}$$

In the homogeneous *w*-core MCF whose cores are arranged in a ring, e.g., 4-core MCF as shown in Fig. 3, *the total crosstalk* in each core is the same and is calculated as

$$P_{XT} = \sum_{\substack{j=1 \\ j \neq i}}^{w} P_{ij} = \sum_{\substack{j=1 \\ j \neq i}}^{w} XT_{ij} P_{orB} \text{ , (15)}$$

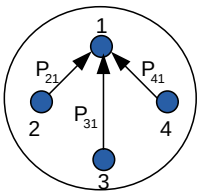


Figure 3. Crosstalk in 4-core MCF.

The optical signal outputting from each core of MCF is converted to electrical signals. Besides the signal current, there also noise current appearing at the output of APDs. Noise current is contributed from several noise components, which can be modeled as additive Gaussian noise, including signal dependent shot noise, inter-core crosstalk-induced shot noise, thermal noise, and also the optical beat noise caused by the beating between the desired signal and the crosstalk one. Consequently, the total noise power after each APD can be calculated as

$$\sigma_{rB}^2 = \sigma_s^2 + \sigma_{XT}^2 + \sigma_{sig-XT}^2 + \sigma_{th}^2 + \sigma_{ASE}^2 + \sigma_{sig-ASE}^2 + \sigma_{XT-ASE}^2 \text{ , (16)}$$

where σ_s^2, σ_{XT}^2, σ_{sig-XT}^2, σ_{th}^2 are the variance of shot and dark noise, crosstalk, beat noise, and thermal noise, respectively. These variances of the noise components can be expressed as

$$\sigma_s^2 = 2qM^2 F_A B(\Re P_{or} + I_d + \Re P_{XT} + \Re P_{ASE}) \text{ , (17)}$$

$$\sigma_{XT}^2 = (\Re P_{XT})^2 \text{ , (18)}$$

$$\sigma_{sig-XT}^2 = 4\Re^2 P_{or} P_{XT} \cos^2 \beta L \text{ , (19)}$$

$$\sigma_{th}^2 = \frac{4K_B T}{R_L} B \text{ , (20)}$$

$$\sigma_{sig-ASE}^2 = 2\Re^2 P_{or} \left[n_{sp}(M-1) h f_0 B_0 \right] \text{ , (21)}$$

$$\sigma_{XT-ASE}^2 = 2\Re^2 P_{XT} \left[n_{sp}(M-1) h f_0 B_0 \right] \text{ , (22)}$$

where q is the electronic charge, B is the effective noise bandwidth, I_d is the dark current, K_B is the Boltzmann constant, T is the temperature of the receiver, R_L is the load resistance. B_0, n_{sp}, h, f_0 are the bandwidth of optical signal, spontaneous emission factor, planks constant and frequency of light wave respectively. F_A is the excess noise factor of the APD. Here, F_A is given by [19] as below,

$$F_A(M_A) = k_A M_A + (1-k_A)(2-1/M_A), \text{ (23)}$$

where k_A is the ionization-coefficient ratio.

Next, the demodulated signal is passed through a dual-threshold direct-detection, which decides bits “0", “1", or “x" as shown in Figure 2.

3.1 Quantum bit error rate

The quantum bit error rate (QBER) is defined as the ratio between the probability that Bob wrongly detect bits “0" and “1" (P_{err}) the probability that Bob is able to detect bits “0" and “1" (P_{sift}) [20]. Accordingly, it can be expressed as

$$\text{QBER} = \frac{P_{err}}{P_{sift}} \text{ , (24)}$$

where, P_{err} and P_{sift} are calculated as

$$\begin{aligned} P_{err} &= P_{A,B}(0,1) + P_{A,B}(1,0) \\ P_{sift} &= P_{A,B}(0,0) + P_{A,B}(0,1) + P_{A,B}(1,0) + P_{A,B}(1,1) \end{aligned} \text{ , (25)}$$

where $P_{A,B}(\mathrm{i},\mathrm{j})$ is the joint probability that Alice’s bit “*i*” coincides with Bob’s bit “*j*”. This probability can be expressed as $P_{A,B}(\mathrm{i},\mathrm{j}) = P_A(i) P_{(B|A)}(i,j)$, where $P_A(i) = 1/2$ and $P_{(B|A)}(i,j)$ is the probability that Bob decides bit “*j*” while Alice sends bit “*i*”. We denote d_0 and d_1 as the detection thresholds for bits “0" and bit “1", respectively. They can be selected symmetrically over the “zero” level. Based on dual-threshold principle, the closed-form expressions for $P_{(B|A)}(i,j)$ can be expressed as

$$\begin{aligned} P_{B|A}(0|0) &= \frac{1}{\sigma_n\sqrt{2\pi}} \int_{-\infty}^{d_0} \exp\left(-\frac{(y-i_0)^2}{2\sigma_n^2} \right) dy = \frac{1}{2} \operatorname{erfc}\left(\frac{i_0 - d_0}{\sigma_n \sqrt{2}} \right) \\ P_{B|A}(0|1) &= \frac{1}{\sigma_n\sqrt{2\pi}} \int_{-\infty}^{d_0} \exp\left(-\frac{(y-i_1)^2}{2\sigma_n^2} \right) dy = \frac{1}{2} \operatorname{erfc}\left(\frac{i_1 - d_0}{\sigma_n \sqrt{2}} \right) \\ P_{B|A}(1|0) &= \frac{1}{\sigma_n\sqrt{2\pi}} \int_{d_1}^{\infty} \exp\left(-\frac{(y-i_0)^2}{2\sigma_n^2} \right) dy = \frac{1}{2} \operatorname{erfc}\left(\frac{d_1 - i_0}{\sigma_n \sqrt{2}} \right) \\ P_{B|A}(1|1) &= \frac{1}{\sigma_n\sqrt{2\pi}} \int_{-\infty}^{d_0} \exp\left(-\frac{(y-i_1)^2}{2\sigma_n^2} \right) dy = \frac{1}{2} \operatorname{erfc}\left(\frac{d_1 - i_1}{\sigma_n \sqrt{2}} \right) \end{aligned} \text{ ,(26)}$$

To adjust the value of two detection thresholds, we define the dual-threshold scale coefficient k as follows

$$\begin{aligned} d_0 &= E[i_0] - k\sqrt{\sigma_n^2} \\ d_1 &= E[i_1] + k\sqrt{\sigma_n^2} \end{aligned} \text{ , (27)}$$

where $E[i_0]$ and $E[i_1]$ are the mean values of i_0 and i_1.

3.2 Egodic Secret Key Rate

Egodic secret key rate, denoted as SKR, shows the security level of the proposed system. The secret key rate is defined as the maximum transmission rate at which Eve is unable to decode any information, written as

$$SKR = I(A;B) - I(A;E) \text{ , (28)}$$

where $I(A;B)$ and $I(A;E)$ are the amount of information shared between Alice and Bob, and between Alice and Eve respectively. With assumption that the probabilities of transmitting bits "0" and "1" are equally likely to occur, the mutual information between Alice and Bob could be calculated as [20]

$$I(A;B) = p\log_2(p) + (1-p-q)\log_2(1-p-q) - (1-q)\log_2(1-q) + 1 - q, \quad (29)$$

where $p = P_{A,B}(0,0) = P_{A,B}(1,1)$ and $q = P_{A,B}(0,x) = P_{A,B}(1,x) = 0.5 - P_{A,B}(0,0) - P_{A,B}(0,1)$.

The mutual information between Alice and Eve could be calculated as [16]

$$I(A;E) = 1 + p_e\log_2(p_e) + (1-p_e)\log_2(1-p_e), \quad (30)$$

where p_e is the probability that Eve correctly detects the transmitted bits from Alice, which can be calculated as $p_e = 0.5 - P_{A,E}(0,1) = 0.5 - P_{A,E}(1,0)$. In addition, Eve's error probability (or QBER) is given as

$$\mathrm{QBER}_{Eve} = P_{A,E}(0,1) + P_{A,E}(1,0), \quad (31)$$

where $P_{A,E}(0,1)$ and $P_{A,E}(1,0)$ are the error probabilities that Eve falsely decides the received bits from Alice. Assuming that Eve uses single-threshold detection, which is often equipped in a typical optical receiver. The error probabilities can be derived as [21]

$$P_{A,E}(0,1) = P_A(0)P_{E|A}(1|0) = \frac{1}{4}\mathrm{erfc}\left(\frac{d_E - i_0}{\sigma_n\sqrt{2}}\right)$$
$$P_{A,E}(1,0) = P_A(1)P_{E|A}(0|1) = \frac{1}{4}\mathrm{erfc}\left(\frac{i_1 - d_E}{\sigma_n\sqrt{2}}\right), \quad (32)$$

where $d_E = 0$ is the threshold detection at Eve's receiver.

IV. NUMERICAL RESULTS

In this section, the performance in terms of QBER and SKR, of the proposed system, based on the performance analysis in Section III, will be analyzed as a function of a number of system parameters including the optical transmitted power (P_t), the D-T scale threshold coefficient, core pitch, the optical fiber length from Alice to Bob. In addition, in this study, we also consider the QBER at Eve (the eavesdropper) to confirm the secure of the system. The system parameters and the propagation characteristics are gathered in Table 1.

Table 1. Key System Parameters

Name	Symbol	Value
Constants and general parameters		
Boltzmann's constant	K	1.38×10^{-23} $WHz^{-1}K^{-1}$
Electronic charge	q	1.6×10^{-19} C
Light velocity	c	3×10^{8} m/s
Load resistance	R_L	50 Ω
Bit rate	R_b	1 Gbps
Temperature	T	300 K
Wavelength	λ	1550 nm
Noise figure	F_n	5 dB
Optical transceiver's parameters		
Modulation index	m	0.2 A/W
Fiber attenuation coefficient	α	0.2 dB/km
PD responsivity	ℜ	0.6 A/W
Ionization-coefficient ratio	k_A	0.7
FWHM linewidth of the laser	$\Delta\upsilon_m$	12.75 MHz
Coupling coefficient	κ	0.02
Bending radius	R_{bd}	0.1 m
The propagation constant	β	rad/micromet

The dual-threshold scale coefficient is one of the most important parameters that network operators need to consider when they design the system. Therefore, in figure 4, the quantum QBER and P_{sift} are presented as a function of the D-T scale coefficient at Bob's receiver. P_{sift} should be larger or equal to 10^{-2} so that Bob can receive the sifted-key from Alice at Mbps with the transmission rates at Gbps. In addition, QBER is kept lower or equal to 10^{-3} so that bit errors are able to be corrected thanks to error correction codes. As shown in Figure 4, in order to meet the above-mentioned targets, the D-T scale threshold should be larger than 3 in case of using 4 core multicore fiber, and in the range of 3 and 5.2 in case of using 61 core multicore fiber. The difference in the D-T scale coefficients is because of the large crosstalk in 61 core MCF.

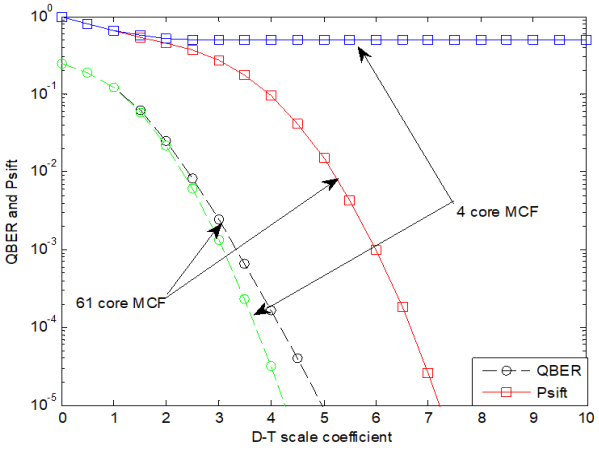


Figure 4. QBER and Psift versus D-T scale coefficient with P_t = -5 dB, L = 50 km

Next, in order to understand how the optical fiber length from Alice to Bob, L, effects on the system performance, we investigate QBER at Bob versus the optical distance with P_t = -5 dBm, M_A = 3, k = 5 in Figure 5. It is apperant from this figure that to keep QBER lower or equal to 10^{-3}, Bob's receiver can be located anywhere when using 4 core MCF, while the location of Bob's receiver should be avoid at the distance of 12-15 km or 20-25 km.

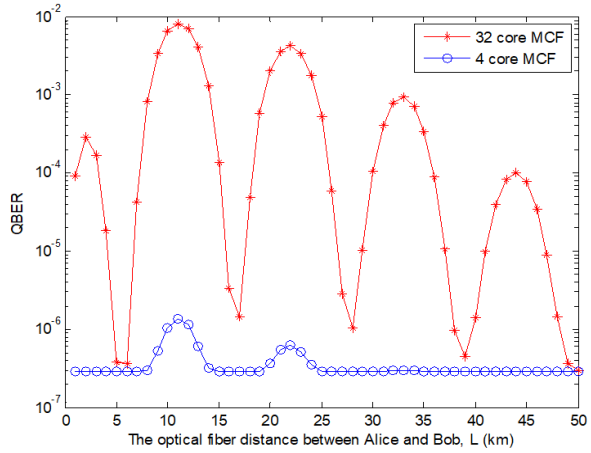


Figure 5. QBER versus the optical distance between Alice and Bob with P_t = -5 dBm, M_A = 3, k = 5.

In figure 6, we investigate the security level of the proposed system versus the transmitted optical power when k = 5, L_1 = 5 km, L = 50 km, M_A = 3. The secret key rate is defined as the maximum transmission rate at which Eve is unable to decode any information. Therefore, the goal of QKD system design is to achieve high ergodic secret-key rate. The results, as illustrated in figure 6, indicate that the secret-key rate of the proposed system is rather high in both cases of MCFs. However, the maximum secret-key rate of the QKD system using 32 core MCF is only 0.422 bit/s/Hz, while the maximum rate of the QKD system using 4 core MCF is 0.5 bit/s/Hz.

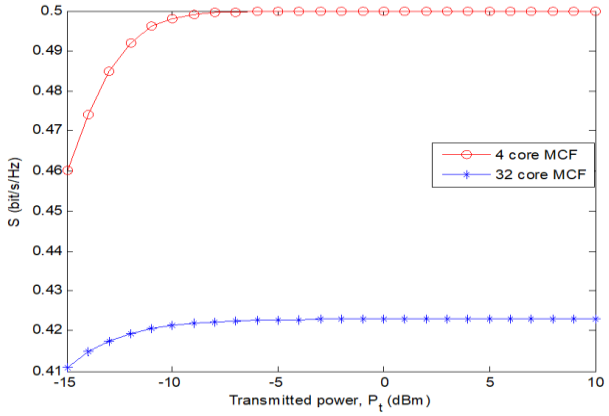


Figure 6. Secret key rate versus the transmitted power with L_1 = 5 km, L = 50 km, M_A = 3, k = 5.

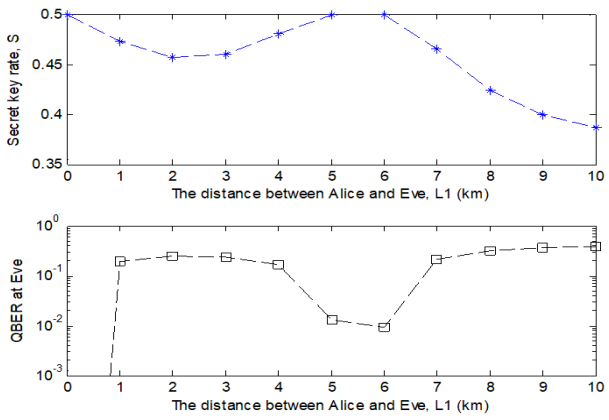


Figure 7. Ergodic secret-key rate and Eve's QBER versus the distance between Alice and Eve using 4 core MCF with P_t = -5 dBm, L = 50 km, k = 5.

Next, ergodic secret-key rate and Eve's QBER are investigated versus the distance between Alice and Eve using 4 core MCF with P_t = -5 dBm, L = 50 km, k = 5. It is clear that both the ergodic secret-key rate and the Eve's QBER fluctuates when the distance between Alice and Eve increases. The goal of QKD system design is to achieve high ergodic secret-key rate while keep Eve's QBER large enough, i.e., larger than 10^{-1}, so that Eve cannot correct the errors by using the error correction codes. To obtain this goal, the distance between Alice and Eve should be smaller than 1 km, or in the range of 4 km and 7 km as can be seen in figure 7. A possible explanation for these results may be that the beat noise is a function of cosine of the distance, as shown in equation (19).

This study also set out with the aim of assessing the importance of using multicore fiber to provide higher security level for the system. Figure 8 below compares the quantum bit error rate at Eve in both using single mode fiber and using 4 core MCF. It is apparent from this figure that there is a significant difference in Eve's QBER even though the transmitted power from Alice is lower than -5 dBm. Moreover, if multicore fiber is used, QBER at Eve could be higher than 10^{-2}. In other words, multicore fibers should be used to help QKD systems safer.

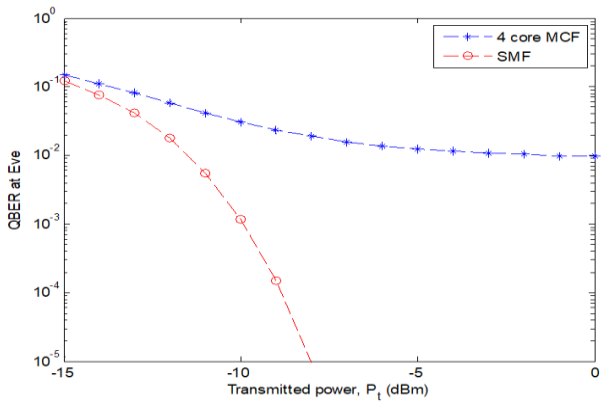


Figure 8. QBER at Eve versus the transmitted power with L_1 = 5 km, M_A = 3, k = 5.

V. CONCLUSIONS

The main goal of the current study was to propose the CV-QKD system using MCF for increasing the secret key rate by transmitting multiple spatial modes simultaneously and also evaluate the deployment capability of the system. In this paper, we have developed a mathematical model of the proposed sysem. We investigated the quantum bit error rate and ergodic secret-key rate versus various system's parameters including the optical fiber length, D-T scale coefficient, transmitted power, core pitch of MCF, crosstalk and receiver noise. The numerical results demonstrated that the proposed system can achieve the desired security

targets including QBER that lower than 10^{-3} and the sifted-key at Mbps. Besides, it is possible to obtain high ergodic secret-key rate of nearly 0.5 while keeping Eve's QBER larger than 10^{-1}. The findings of this study suggest that the CV-QKD system is an effective solution to distribute the quantum key with more secure and higher secret key rate.

REFERENCES

[1] L.-J. Wang, K.-H. Zou, W. Sun, Y. Mao, Y.-X. Zhu, H.-L. Yin, Q. Chen, Y. Zhao, F. Zhang, T.-Y. Chen, and J.-W. Pan, ''Long-distance copropagation of quantum key distribution and terabit classical optical data channels,'' Phys. Rev. A, Gen. Phys., vol. 95, no. 1, Jan. 2017, Art. no. 012301.

[2] S. Kleis, J. Steinmayer, R. H. Derksen, and C. G. Schaeffer, ''Experimental investigation of heterodyne quantum key distribution in the S-Band embedded in a commercial DWDM system,'' in Proc. Opt. Fiber Commun. Conf.(OFC), 2019, pp. 1–3, Paper. Th1J.3.

[3] F. Karinou, H. H. Brunner, C.-H.-F. Fung, L. C. Comandar, S. Bettelli, D. Hillerkuss, M. Kuschnerov, S. Mikroulis, D. Wang, C. Xie, M. Peev, and A. Poppe, ''Toward the integration of CV quantum key distribution in deployed optical networks,'' IEEE Photon. Technol. Lett., vol. 30, no. 7, pp. 650–653, Apr. 1, 2018.

[4] P. J. Winzer, ''Spatial multiplexing in fiber optics: The 10X scaling of Metro/Core capacities,'' Bell Labs Tech. J., vol. 19, pp. 22–30, Sep. 2014.

[5] R. S. Luís, B. J. Puttnam, J. M. D. Mendinueta, W. Klaus, J. Sakaguchi,Y. Awaji, T. Kawanishi, A. Kanno, and N. Wada, ''OSNR penalty of selfhomodyne coherent detection in spatial-division-multiplexing systems,'' IEEE Photon. Technol. Lett., vol. 26, no. 5, pp. 477–479, Mar. 1, 2014.

[6] X. Pang, ''High-speed SDM interconnects with directly-modulated .5-μm VCSEL enabled by low-complexity signal processing techniques,'' in Proc. Signal Process. Photon. Commun., vol. 2018, pp. 1–2, Paper. Sp

[7] J. F. Dynes, S. J. Kindness, S. W.-B. Tam, A. Plews, A. W. Sharpe, M. Lucamarini, B. Fröhlich, Z. L. Yuan, R.V. Penty, and A. J. Shields, "Quantum key distribution over multicore fiber," Opt. Express 24(8), 8081-8087 (2016).

[8] G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. W. R. Connolly, A. Przysiezna, E. S. Gómez, M. Figueroa, . Vallone, P. Villoresi, T. Ferreira da Silva, G. B. Xavier, and G. Lima, "High-dimensional decoystate quantum key distribution over multicore telecommunication fibers," Phys. Rev. A 96, 022317 (2017).

[9] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, "High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits," npj Quantum Information 3, 25 (2017).

[10] T. A. Eriksson et al., "Coexistence of continuous variable quantum key distribution and 7×12.5 Gbit/s classical channels," in Proc. IEEE Photon. Soc. Summer Top. Meeting Ser. (SUM), Jul. 2018, pp. 71–72.

[11] F. Li, H. Zhong, Y. Wang, Y. Kang, D. Huang, and Y. Guo, "Performance analysis of continuous-variable quantum key distribution with multi-core fiber," Appl. Sci., vol. 8, no. 10, p. 1951, 2018.

[12] Tobias A. Eriksson , Benjamin J. Puttnam,..., "Crosstalk Impact on Continuous Variable Quantum Key Distribution in Multicore Fiber Transmission," IEEE PHOTONICS TECHNOLOGY LETTERS, VOL. 31, NO. 6, MARCH 15, 2019

[13] Thu A. Pham, Nga T. T. Nguyen, and Ngoc T. Dang, "Quantum Key Distribution over Hybrid Fiber-Wireless System for Mobile Networks" In the Proc. of the ACM Eighth International Symposium on Information and Communication Technology (SoICT 2019), Hanoi-Halong, Vietnam, Dec. 2019, pp. 236-241.

[14] T Hayashi, T Taru, O Shimakawa, T Sasaki, E Sasaoka, Design and fabrication of ultra-low crosstalk and low-loss multi-core fiber, Optics express, Vol.19, No.17, 2011.

[15] Masanori Koshiba, Kunimasa Saitoh, Katsuhiro Takenaga, and Shoichiro Matsuo, "Multi-core fiber design and analysis: coupled-mode theory and coupled-power theory," Opt. Express 19, B102-B111 (2011).

[16] M. Koshiba, K. Saitoh, K. Takenaga, and S. Matsuo, "Multi-core fiber design and analysis: coupled mode theory and coupled-power theory," Optics Express, vol.19, no.16, pp.B102-B111, 2011.

[17] D. Marcuse, "Derivation of coupled power equations," Bell Syst. Tech. J. 51, 229–237, 1972.

[18] Ahmed E. A. Farghal, Performance analysis of core-multiplexed spectral amplitude coded OCDMA PON, Journal of Optical Communications and Networking, Vol. 8, Iss. 9, Sept. 2016.

[19] Govind P. A. Fiber-Optic Communications Systems. John Wiley & Sons 2002, Third Edition, Inc. ISBNs: 0-471-21571-6 (Hardback); 0-471-22114-7 (Electronic).

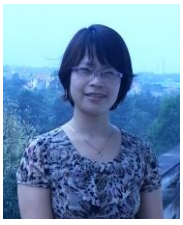
[20] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography" Rev. Mod. Phys., vol. 74, pp. 145–195, 2002

[21] P. V. Trinh, T. V. Pham, N. T. Dang, H. V. Nguyen, S. X. Ng and A. T. Pham, "Design and security analysis of quantum key distribution protocol over free-space optics using dual-threshold direct-detection receiver," IEEE Access, vol. 6, pp. 4159–4175, 2018.

PHÂN TÍCH HIỆU NĂNG HỆ THỐNG CV-QKD SỬ DỤNG SỢI QUANG ĐA LÕI

Tóm tắt: Trong bài báo này, chúng tôi đã đề xuất một hệ thống phân phối khóa lượng tử (QKD) sử dụng sợi quang đa lõi (MCF). Sau đó, hiệu năng của hệ thống đề xuất được phân tích về mặt lý thuyết dưới ảnh hưởng của nhiều tham số lớp vật lý như là nhiễu và xuyên nhiễu của sợi MCF. Tính khả thi của kiến trúc đề xuất được xác minh thông qua các kết quả số. Kết quả mô phỏng chứng minh rằng giải pháp đề xuất có thể nâng cao đáng kể tốc độ khóa bí mật. Nó cũng chỉ ra rằng hiệu năng của hệ thống phụ thuộc rất nhiều vào loại sợi quang đa lõi MCF.

Từ khóa: Phân phối khóa lượng tử (QKD), Sợi quang đa lõi (MCF).



Thu A. Pham received B.E degree of Telecommunication engineering from Posts and Telecommunications Institute of Technology (PTIT), Viet Nam, in 2003, and M.E degree of Telecommunication engineering from Royal Melbourne Institute of Technology, Australia, in 2008. Now, she is a lecturer and PhD student in Telecommunication faculty of PTIT. Her research interests include networking, radio over fiber, and broadband networks.

*Email: thupa@ptit.edu.vn