applied sciences

MDPI

Article

Performance Analysis of Continuous-Variable Quantum Key Distribution with Multi-Core Fiber

Fei Li, Hai Zhong, Yijun Wang, Ye Kang, Duan Huang * and Ying Guo

School of Information Science and Engineering, Central South University, Changsha 410083, China; csulifei@csu.edu.cn (F.L.); haizhong2018@foxmail.com (H.Z.); xxywyj@sina.com (Y.W.); zhsmile99@aliyun.com (Y.K.); yingguo@csu.edu.cn (Y.G.)

* Correspondence: duanhuang@csu.edu.cn

Received: 4 September 2018 ; Accepted: 15 October 2018; Published: 17 October 2018

Abstract: Performance analysis of continuous-variable quantum key distribution (CVQKD) has been one of the focuses of quantum communications. In this paper, we propose an approach to enhancing the secret rate of CVQKD with the multi-core fiber (MCF) system that transmits multiple spatial modes simultaneously. The excess noise contributed by the inter-core crosstalk between cores can be effectively suppressed by quantum channel wavelength management, leading to the performance improvement of the MCF-based CVQKD system. In the security analysis, we perform numerical simulations for the Gaussian-modulated coherent state CVQKD protocol, considering simultaneously the extra insert loss of fan-in/fan-out (FIFO), which is the extra optical device that should be used at the input and the output of the fiber. Simulation results show that the performance of the one-way and two-way protocols for each core are slightly degraded because of the insert loss of the FIFO, but the total secret key rate can be increased, whereas the performance of the measurement-device-independent CVQKD protocol will be degraded due to the effect of the insert loss of the FIFO. These results may provide theoretical foundation for the space-division multiplexing CVQKD system.

Keywords: quantum cryptography; continuous-variable quantum key distribution; multi-core fiber

1. Introduction

Since Bennett and Brassard presented the first quantum key distribution (QKD) protocol, i.e., BB84 protocol [1], lots of groundbreaking researches of QKD have emerged. The previous QKD was based on discrete variable (DV) that encodes information into a single photon state. However, the generation and detection of single photons still remain a significant technology challenge in DVQKD. Fortunately, an alternative approach, continuous-variable (CV) QKD [2], was proposed as it can be compatible with mature components and technologies of classical communication, resulting in high detection efficiency. CVQKD has been proved to be secure against general collective attacks, which are optimal in both the asymptotic case [3,4] and the finite-size regime [5–7]. To lift the security loopholes of the local oscillator (LO) and the detector, the locally generated LO schemes [8–10] and the measurement-device-independent (MDI) schemes [11–13] have been proposed recently. In experiments, long distance of up to 150 km [14], high speed of up to 12 Mbit/s [15] and high security MDI quantum cryptography [16] in CVQKD have also been achieved.

In the last decade, theoretical performance analysis of CVQKD has been suggested [17–24]. Moreover, multiplexing technologies, which are based on wavelength, polarization, phase and orbital angular momentum, have been demonstrated for the CVQKD system to improve its performance [15,25–27]. However, the rate at present is far from meeting the needs of the practical implementation. How to increase the secret key rate is still worthy of further investigation. In the last

few years, to avoid a capacity crunch in the single-mode fiber (SMF), space-division multiplexing (SDM) technique has been proposed to further increase the data bandwidth in classical communications. One realizing approach of SDM is to use multi-core fiber (MCF). Through using it, another multiplexing dimensionality—spatial dimension—is able to be fully utilized to increase the secret key rate. The contained cores of the MCF can be exploited as parallel channels for independent signals and hence the data bandwidth can be multiplied. Recently, experimental demonstration has been made for DVQKD based on the SDM technique over a MCF [28–30], which opens a way for CVQKD to break through the bottleneck of the secret key rate in the traditional SMF-based system.

In this paper, we propose the MCF-based CVQKD scheme, which can increase the secret key rate via transmitting multiple spatial modes simultaneously. The excess noise contributed by the inter-core crosstalk between cores can be effectively suppressed by using quantum channel wavelength management between cores. As extra optical devices of the fan-in/fan-out (FIFO) should be used at the input and output of the fiber, the insert loss of these devices should also be considered. We perform simulations based on the Gaussian-modulated coherent state CVQKD protocol and numeric results show that the performance of the one-way and two-way protocols for each core may be slightly degraded because of the insert loss of the FIFO, but the total secret key rate can be significantly improved. However, the performance of the MDI CVQKD protocol will be degraded due to the effect of the insert loss of the FIFO.

This paper is arranged as follows. In Section 2, we show the channel characteristic of the MCF-based CVQKD. In Section 3, we present the performance analysis of the MCF-based CVQKD protocols in terms of the secure key rate. Finally, we draw conclusion in Section 4.

2. The MCF-Based CVQKD

The MCF constrains several cores in the same cladding, where each core can be seen as a single SMF transmitting signals independently. Compared with the SMF, all the cores in the MCF can be exploited as parallel SMFs for independent signals so that the communication capacity can grow exponentially. Figure 1a shows a common 7-core MCF. However, this multi-core structure will bring out some challenges. For example, extra optical devices, fan-in and fan-out, must be inserted at the input and output of the MCF. The insert loss of these components should not be neglected. In addition, the electric field of mode in each core is not completely confined to the core, but part of the cladding, as shown in Figure 1a. Consequently, as all the cores are confined in the same cladding, the electric field at each wavelength in the individual core of MCF will transfer into adjacent cores through evanescent field coupling, as shown in Figure 1b. As a result, the inter-core crosstalk, which has the same wavelength with the launched signal, is generated. Usually, the CVQKD system is sensible with the magnitude of excess noise. The inter-core crosstalk between cores may increase the excess noise and then degrade the performance of the CVQKD system. Therefore, the impact contributed from the inter-core crosstalk should be taken into account. It will be accumulated linearly along the fiber length, which can be attributed to randomly perturbation caused by fiber imperfection [31]. Its magnitude depends on fiber length and coupling coefficient, which is determined by fiber bend, fiber twist, the electric field differential propagation constant $\delta\beta$ of two cores, core pitch, mode coupling coefficient and correlation length [31–33]. As described in [32], the inter-core crosstalk XT_{mn} from core m to core n can be evaluated by

$$XT_{mn} = \tanh(\overline{h}_{mn}L), \tag{1}$$

where $\overline{h}_{mn}$ is the coupling coefficient between core m and core n, and L is the transmission distance. XT_{mn} should be understood as the output power ratio of core n to core m. The leakage power contributed from the inter-core crosstalk from core m to core n can be estimated in power by $P_{XT}^{mn}(L) = XT_{mn}TP_m(0)$ with $T = 10^{-\alpha L}$, where $P_m(0)$ is the input power of core m, T is the

transmittance of the fiber, and α is the fiber loss coefficient. In mean photon number, the formula above can be rewritten as

$$\langle \hat{N}_{XT}^{mn}(L) \rangle = XT_{mn}T\langle \hat{N}^{m}(0) \rangle = \tanh(\bar{h}_{mn}L)\langle \hat{N}^{m}(L) \rangle, \tag{2}$$

where $\langle \hat{N}^{m}(0) \rangle$ is the input mean photon number of the core m, and $\langle \hat{N}^{m}(L) \rangle$ is the output mean photon number of the core m.

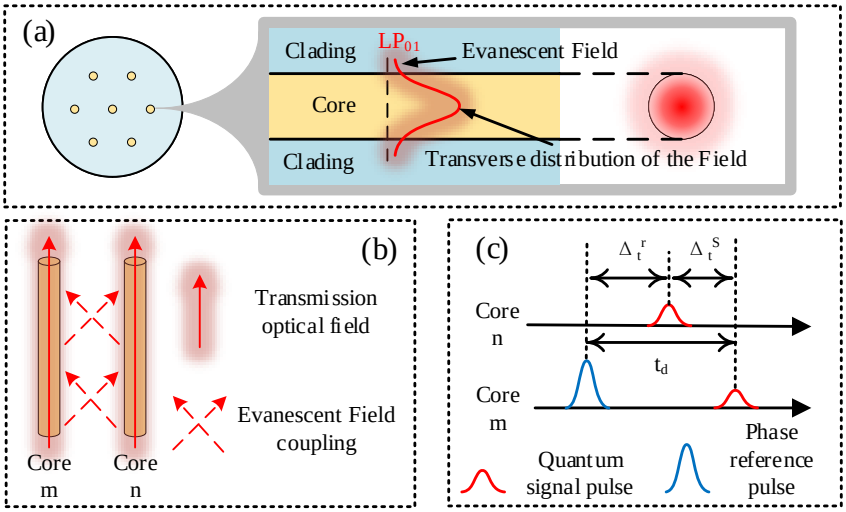

Figure 1. Multi-core fiber and the illustration of inter-core crosstalk. (**a**) A common 7-core MCF and the transverse distribution of the optical field in a single core. (**b**) The inter-core crosstalk between two cores. (**c**) The time delay of pulses between two cores. Δ_t^r is the time delay between the phase reference pulse in core m and the most nearby quantum signal pulse in core n. Δ_t^s is the time delay between the quantum signal pulse in core m and the most nearby quantum signal pulse in core n. t_d is the time delay between quantum signal pulse and phase reference pulse in the same core and $t_d = \Delta_t^s - \Delta_t^r$. We assume $\Delta_t^r < 0$ for the case in (**c**).

If the above inter-core crosstalk has the same wavelength with the quantum signals, it will contribute to the in-band excess noise as it is in the same spatiotemporal mode as the LO of the core n, where the LO is generated locally or transmitted with quantum signal. The CVQKD systems at present are all pulse system. In order to estimate the above excess noise, we consider the impact of the adjacent cores' quantum signal pulses and phase reference pulses, which are overlapped temporally with the quantum signal pulse in the interested core. Figure 1c shows the time delay between one core's quantum signal pulse and the adjacent core's quantum signal pulse and phase reference pulse. Therefore, assuming the wavelength of quantum channels in core m and core n are equal, the excess noise contributed by the inter-core crosstalk from core m to core n referred to the input can be given by

$$\xi_{XT} = \xi_{XT}^{ref} + \xi_{XT}^{sig} \tag{3}$$

with

$$\xi_{XT}^{ref} = \frac{1}{2}\frac{\eta_F\eta \cdot 2\langle \hat{N}_{ref}^{out} \rangle \tanh(\bar{h}_{mn}L)}{T\eta_F\eta} \sum_{k=-1}^{1} e^{-\frac{(\Delta_t^r - \frac{k}{R})^2}{2\sigma_t^2}} = \frac{\langle \hat{N}_{ref}^{out} \rangle \tanh(\bar{h}_{mn}L)}{T} \sum_{k=-1}^{1} e^{-\frac{(\Delta_t^r - \frac{k}{R})^2}{2\sigma_t^2}}, \tag{4}$$

$$\xi_{XT}^{sig} = \frac{1}{2}\frac{\eta_F\eta \cdot 2\langle \hat{N}_{sig}^{out} \rangle \tanh(\bar{h}_{mn}L)}{T\eta_F\eta} \sum_{k=-1}^{1} e^{-\frac{(\Delta_t^s - \frac{k}{R})^2}{2\sigma_t^2}} = \frac{\langle \hat{N}_{sig}^{out} \rangle \tanh(\bar{h}_{mn}L)}{T} \sum_{k=-1}^{1} e^{-\frac{(\Delta_t^s - \frac{k}{R})^2}{2\sigma_t^2}}, \tag{5}$$

where Δ_t^r is the time delay between the phase reference pulse in core m and the most nearby quantum signal pulse in core n, Δ_t^s is the time delay between the quantum signal pulse in core m and the most nearby quantum signal pulse in core n, σ_t is the half-width of the pulse (at 1/e-intensity point), $e^{-(\Delta_t^r - k/R)^2/2\sigma_t^2}$ and $e^{-(\Delta_t^s - k/R)^2/2\sigma_t^2}$ are the overlapping factor [34], $\langle \hat{N}_{ref}^{out} \rangle$ is the mean photon number of the phase reference pulse in the core m, $\langle \hat{N}_{sig}^{out} \rangle$ is the mean photon number of the quantum signal pulse in the core m, ξ_{XT}^{ref} is the excess noise contributed by the phase reference pulses, ξ_{XT}^{sig} is the excess noise contributed by the quantum signal pulses, R is the repetition rate of CVQKD system, η_F is the insert loss of the FIFO, η is the detector quantum efficiency. We only consider the adjacent 3 quantum signal pulses and phase reference pulses (corresponding to $k = -1, 0, 1$), and others' impact can be neglected as the overlapping factor will be too low. The phase reference pulse would be the LO pulse or the weak reference pulse [8–10]. We assume that all the pulses are the Gaussian pulse shape with the same pulse width. Note, as the coupling between cores occur randomly, the polarization state of the crosstalk will be randomized and chaotic. Consequently, there is a factor of 1/2 in Equations (4) and (5) due to the polarization selection of the LO. According to Equation (4), we show the excess noise contributed from the weak reference pulses in Figure 2, where the pulse width is 50 ns, α is 0.2 dB/km, R is 1 MHz and the coupling coefficient takes an ultra-low value of −90 dB/km [31]. Usually, the mean photon number of the weak reference pulse is about 100∼1000 at the fiber output. Therefore, the resulting excess noise contributed from the weak reference pulse cannot be neglected when Δ_t^r approaches to zero. We do not show the impact of the quantum signal pulse as its impact is much lower than the weak reference pulse's, although the quantum signal pulse's impact will be non-negligible when $h_{mn} \geq -80$ dB/km, $\langle N_{sig}^{out} \rangle = 10$ and $\Delta_t^s = 0$. We also do not show the contribution of the LO, as its mean photon number (10^8 as usual) is much larger than the weak reference pulse so that its excess noise contribution is unbearable. Consequently, the excess noise contributed by the inter-core crosstalk may become very large for the MCF-based CVQKD when the wavelengths of quantum channels in all cores are equal, even though the using of the ultra-low crosstalk MCF. In practice, for the improvement of the communication capacity, we should use a smaller core pitch and hence more cores MCF, leading to a larger coupling coefficient. Therefore, an effective suppression of the impact of the inter-core crosstalk can increase the secure key rate of MCF-based CVQKD system. Note, the calculations above assume that the time delay of Δ_t^r and Δ_t^s between pulses are invariable. This assumption may not follow the real situation when we use heterogeneous MCF, but this does not affect our analysis above as we can use an average value to take the estimation.

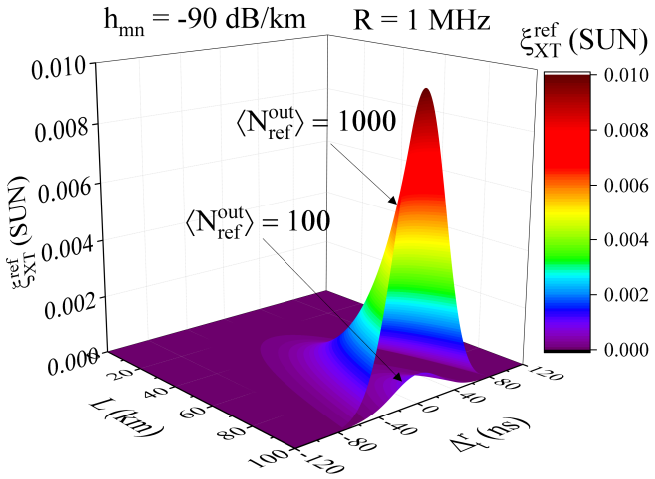

Figure 2. The excess noise contributed from the weak reference pulse as a function of the transmission distance and Δ_t^r. SUN, shot noise units.

To suppress the impact of the inter-core crosstalk to the quantum channel, we consider this problem in three points. First, we can monitor pulses time delay between cores constantly. This method is feasible for few-core and low-speed MCF-based CVQKD system as the pulse period is large and the adjacent cores of one core is few. However, this approach will increase the system's cost, which is increased with the system's core number and the repetition rate. Therefore, it is not a good solution. Second, we consider using a low coupling coefficient MCF so that the excess noise contributed by the inter-core crosstalk is lower than $0.001N_0$ (N_0 is the shot noise), and hence this excess noise can be neglected [35]. This method is straightforward. However, it will bring about challenges of MCF fabrication technique or decrease the total communication capacity of the system. Take the central core of a 7-core MCF for example. For the transmitted LO scheme, the coupling coefficient should be lower than -157 dB/km when the output mean photon number of the LO is 10^8. It is so hard to fabricate a so low coupling coefficient MCF, when maintaining a relatively small core pitch (45 μm for example [31]). For the locally generated LO scheme, the conservative value of the coupling coefficient should be lower than -107 dB/km when the mean photon number of the weak phase reference pulse is 1000. The fabrication of this value of coupling coefficient for MCF is also a challenge. Actually, one can increase the core pitch to decrease the coupling coefficient of MCF, but this approach will also decrease the core density of MCF and degrade the total communication capacity indirectly. Therefore, using a low coupling coefficient MCF to remove the impact of inter-core crosstalk is not preferred in practice. Note, the excess noise should be the sum of all the adjacent cores' contributions, and the conservative estimation of the coupling coefficient above is under the assumption of $\Delta_t^r = 0$ and $L = 100$ km. Third, we consider staggering the wavelength of quantum channel in each core. If the wavelength of the inter-core crosstalk differs from the wavelength of the quantum channel, it can be removed by filtering technology at the receiver [36]. Moreover, the mode selection of the LO can restrict this noise further [37]. Consequently, this method can be ready to realize in present technology and appears good at noise suppressing. To restrict the impact of the inter-core crosstalk, we propose the channel wavelength distribution scheme in Figure 3, where all the wavelengths of quantum channels are different. Under this condition, the wavelength of the inter-core crosstalk in each core will be different from the wavelength of quantum channel and this crosstalk can be removed out at the receiver. Therefore, a good channel wavelength management can put down the impact of the inter-core crosstalk.

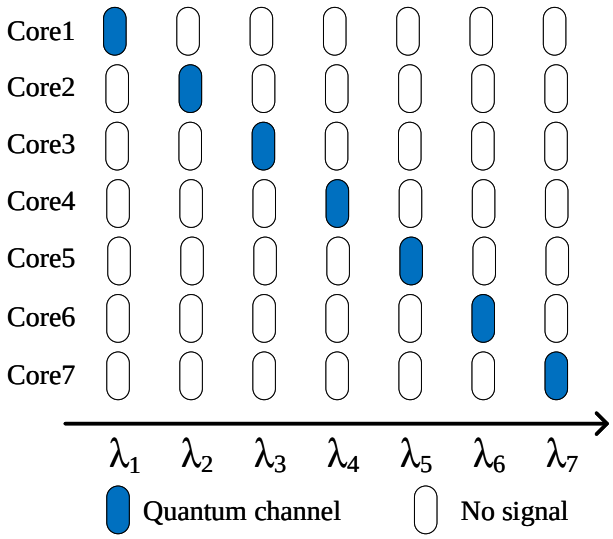

Figure 3. Different distribution of quantum channel wavelength in each core.

3. Performance Analysis

We have demonstrated the characteristics of the MCF-based CVQKD system. Figure 4 depicts the MCF-based CVQKD protocol, including the one-way or two-way CVQKD protocols [8,17] and the MDI CVQKD protocol [38]. The global parameters that are used for simulations are the fiber loss coefficient α and the electronic noise v_{el}, quantum efficiency η of the homodyne detector and the system excess noise ϵ_0, the reconciliation efficiency β and the insert loss of the FIFO η_F. All the above parameters are given in simulations with the values $\alpha = 0.2$ dB/km, $v_{el} = 0.01N_0$, $\eta = 0.719$, $\epsilon_0 = 0.01N_0$, $\beta = 0.95$ and $\eta_F = 1.1$ dB, 0.5 dB or 0 dB, respectively [8,14,28].

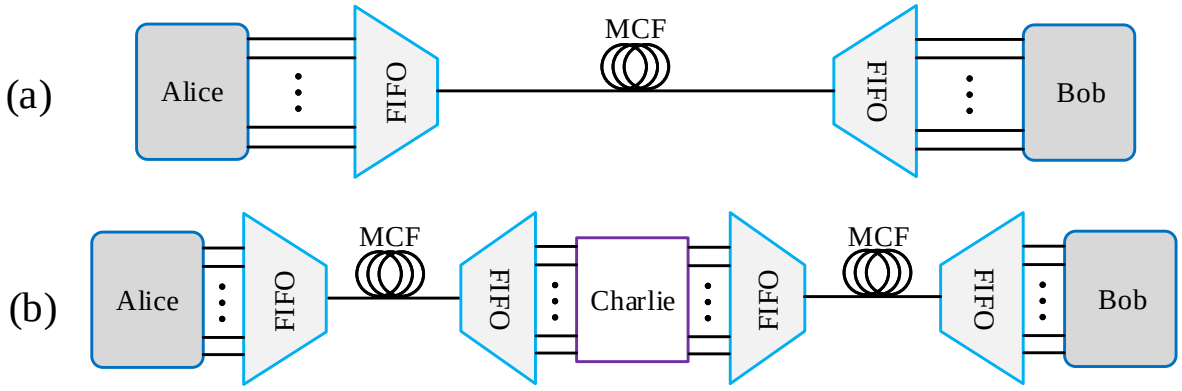

Figure 4. The MCF-based CVQKD protocols. (**a**) The one-way or two-way CVQKD protocol. (**b**) The MDI CVQKD protocol. FIFO: fan-in/fan-out.

For the one-way CVQKD protocol, the secure key rate with reverse reconciliation under collective attacks is given by [8,17]

$$K = \beta I_{AB} - \chi_{BE}, \tag{6}$$

where I_{AB} is the Shannon mutual information between Alice and Bob, and χ_{BE} is the Holevo bound in the information between Bob and Eve. Appendix A gives the calculations of I_{AB} and χ_{BE}. The numerical results of the one-way protocol are shown in Figure 5, where (a) and (b) represent the results of the transmitted LO scheme while (c) and (d) represent the results of the locally generated LO schemes. Here Alice's modulation V_A is set to $4N_0$ and $20N_0$ in Figure 5a,b, and $40N_0$ in Figure 5c,d, respectively. As shown in Figure 5 we find that although the secret key rate of one-core-based CVQKD may be slightly smaller than that of the original SMF-based CVQKD, the total secret key rate is still improved for the MCF-based system. The decreasing secret key rate of one-core-based CVQKD is due to the insert loss of the FIFO. When this insert loss decreases to a threshold, its impact can be nearly neglected, as the violet lines shown in Figure 5a,b, where the insert loss of the FIFO is set to 0.5 dB. We can also find that the insert loss of the FIFO has less influence to the transmitted LO scheme than the locally generated LO scheme, especially when V_A is close to the optimal value of $4N_0$. This result can also be reflected by the simulation of tolerable excess noise. We have shown the tolerable excess noise for one-way protocols in Figure 5e,f, when η_F takes different values. It shows that the locally generated LO scheme is more sensitive to the insert loss of the FIFO. Therefore, with lower insert loss of the FIFO and more cores of MCF, the performance of the MCF-based one-way CVQKD protocols can be improved better. We note that the numerical results of the two-way protocol is similar to that of the one-way protocol, and hence can be ignored for simplicity.

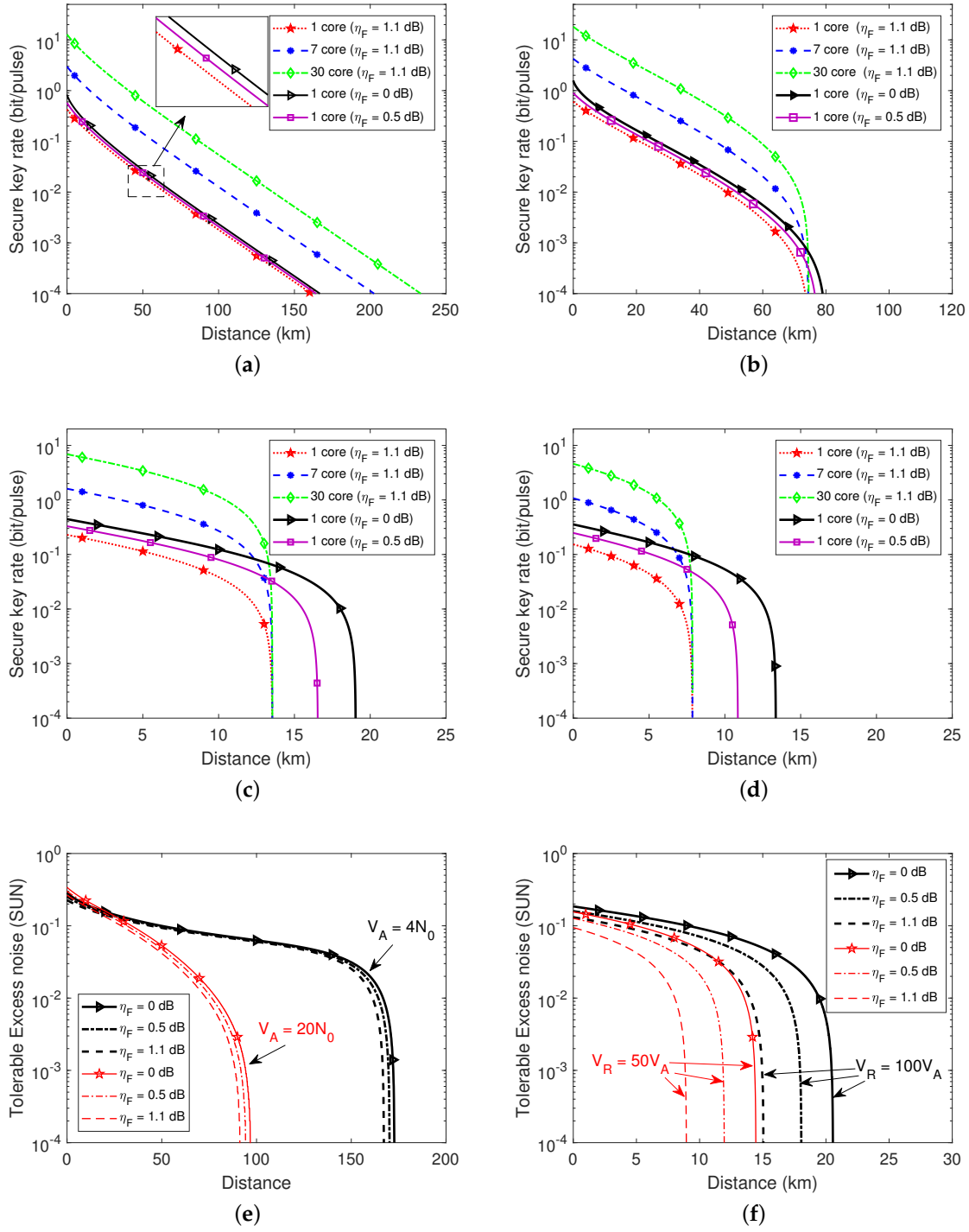

Figure 5. The secret key rate and the tolerable excess noise of MCF-based one-way CVQKD protocols, when using different values of η_F. (**a**) CVQKD with transmitted LO for $V_A = 4N_0$. (**b**) CVQKD with transmitted LO for $V_A = 20N_0$. (**c**) CVQKD with locally generated LO for $V_R = 100V_A$. (**d**) CVQKD with locally generated LO for $V_R = 50V_A$. (**e**) The tolerable excess noise for the transmitted LO scheme. (**f**) The tolerable excess noise for the locally generated LO scheme. V_A is set to $40N_0$ for the locally generated LO scheme. In the results of secret key rate, the black lines are for the SMF-based system, the red dotted lines are for the one-core-based system, the blue lines are for the 7-core-based system and the green dash dotted lines are for the 30-core-based system, the violet solid lines are the results for the case of using SMF, i.e., $\eta_F = 0$ dB.

For the MDI CVQKD protocol, the secret key rate under Gaussian attacks is given by [16]

$$R = g\left(\frac{\tau_A\chi}{\tau_A+\tau_B}-1\right)-g\left[\frac{\tau_A\tau_B\chi-(\tau_A+\tau_B)^2}{|\tau_A-\tau_B|(\tau_A+\tau_B)}\right]+log_2\left[\frac{2(\tau_A+\tau_B)}{e|\tau_A-\tau_B|\chi}\right], \quad (7)$$

where $g(x) = \frac{x+1}{2}log_2\frac{x+1}{2} - \frac{x-1}{2}log_2\frac{x-1}{2}$, $\tau_A = \eta_F 10^{-\alpha L_A/10}$, $\tau_B = \eta_F 10^{-\alpha L_B/10}$, and $\chi = 2(\tau_A+\tau_B)/\tau_A\tau_B + \epsilon_0$. L_A is the distance between Alice and Charlie, and L_B is the distance between Bob and Charlie. However, we could not obtain a positive secret key rate for $\eta_F = 1.1$ dB. The reason is that the insert loss of 1.1 dB is equivalent to an extra distance of 5.5 km, which is equivalent to add 5.5 km initial distance between Alice and Charlie. Unfortunately, the secure distance of the MDI CVQKD protocol will decrease rapidly with the distance between Alice and Charlie [16], which prevents us to obtain a positive secret key rate for $\eta_F = 1.1$ dB. Furthermore, although η_F is set to 0.5 dB or 0.1 dB, the secure transmission distance is also short with $L_A \simeq 0$, as shown in Figure 6, where the reconciliation efficiency is set to 1. In practice. The results in Figure 6 may become even worse since the reconciliation efficiency is not able to achieve 1.

We also show the tolerable insert loss of the FIFO for the MDI scheme in Figure 7, when fixing the distance between Alice and Charlie for difference values. It shows that the secure distance between Alice and Bob is able to reach a longer value of up to 50 km when η_F is low enough. It also shows the shorter L_A is, the larger toleration of η_F can be achieved.

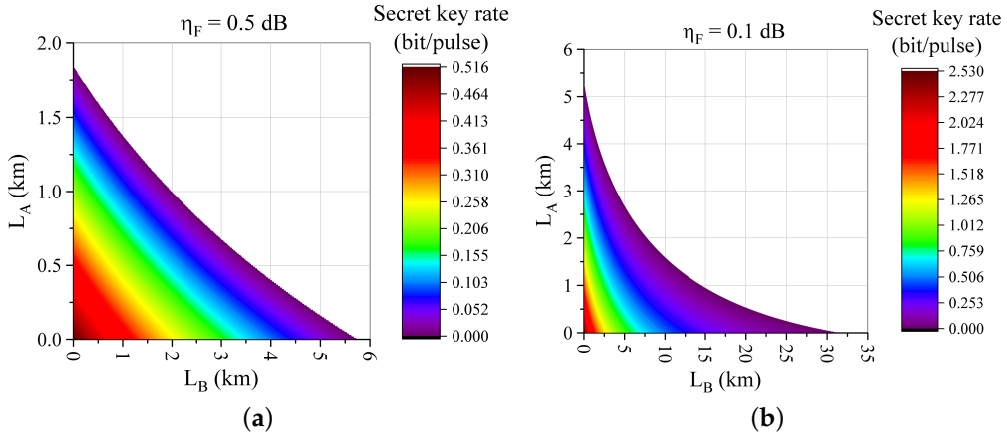

Figure 6. The secret key rate of one core for the multi-core-based MDI CVQKD protocol. (**a**) $\eta_F = 0.5$ dB. (**b**) $\eta_F = 0.1$ dB. η_F is the insert loss of the FIFO. Alice and Bob's modulation are much larger than 1. L_A is the distance between Alice and Charlie. L_B is the distance between Bob and Charlie.

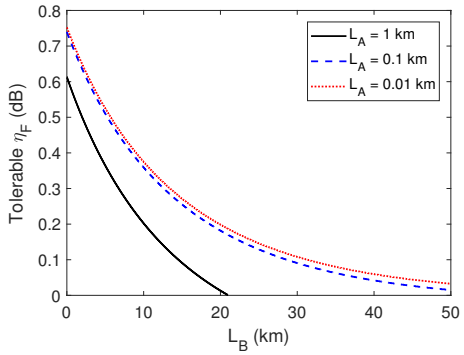

Figure 7. The tolerable insert loss of FIFO when fixing the distance between Alice and Charlie. The black solid line represents the result of $L_A = 1$ km. The blue dashed line represents the result of $L_A = 0.1$ km. The red dotted line represents the result of $L_A = 0.01$ km.

4. Conclusions

We have proposed the performance analysis of the MCF-based CVQKD. The excess noise contributed by the inter-core crosstalk can be effectively suppressed by quantum channel wavelength management between cores. As extra optical devices of FIFO should be used at the input and output of the fiber, the insert loss of these devices should also be considered. In the security analysis, we perform numerical simulations based on the Gaussian-modulated coherent state protocol. Simulation results show that the performance of the one-way and two-way CVQKD protocols for each core are slightly degraded because the insert loss of the FIFO, but the total secret key rate can be improved obviously. The performance of the MDI CVQKD protocol will be degraded because of the insert loss of the FIFO, which can be seen as an equivalent initial distance between Alice and Charlie. These results may provide theoretical foundation for the SDM in the CVQKD system.

Author Contributions: F.L. gave the general idea of the study, designed the conception of the study and performed critical revision of the manuscript. H.Z. accomplished the formula derivation and numerical simulations and drafted the article. Y.W. performed critical revision of the manuscript. Y.K. provided feasible revision of the manuscript. D.H. performed critical revision of the manuscript, provided critical advice and reviewed relevant studies and literatures. Y.G. conceived of and designed the study. All authors have read and approved the final manuscript.

Funding: This research received no external funding.

Acknowledgments: This work was supported by the National Natural Science Foundation of China (Grant Nos. 61572529, 61871407, 61801522).

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. The Secret Key Rate Calculation of the One-Way Protocol

In this section we give the secret key rate calculation of the one-way protocol. The equivalent entanglement-based (EB) description is used to for the security analysis. We first come to the transmitted LO scheme. The mutual information of Alice and Bob can be written as [17]

$$I_{AB} = \frac{1}{2} log_2 \frac{V + \chi_{tot}}{1 + \chi_{tot}} \tag{A1}$$

with

$$\chi_{tot} = \chi_{line} + \chi_h, \tag{A2}$$

$$\chi_{line} = \frac{1 - T_c}{T_c} + \epsilon_0, \tag{A3}$$

$$\chi_h = \frac{(1 - \eta) + v_{el}}{\eta}, \tag{A4}$$

where $V = V_A + 1$ and V_A is the modulation variance of Alice, $T_c = \eta_F T$. The Holevo bound in the information between Bob and Eve can be given by

$$\chi_{BE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{A5}$$

where $G(x) = (x + 1) log_2(x + 1) - x log_2 x$. The symplectic eigenvalues $\lambda_{1,2}$ and $\lambda_{3,4}$ are given by

$$\lambda_{1,2}^2 = \frac{1}{2}[A \pm \sqrt{A^2 - 4B}], \tag{A6}$$

$$\lambda_{3,4}^2 = \frac{1}{2}[C \pm \sqrt{C^2 - 4D}], \tag{A7}$$

with

$$A = V^2(1-2T_c)+2T_c+(T_c)^2(V+\chi_{line}), \quad \text{(A8)}$$

$$B = T_c^2(V\chi_{line})^2, \quad \text{(A9)}$$

$$C = \frac{A\chi_h + V\sqrt{B} + T_c(V+\chi_{line})}{T_c(V+\chi_{tot})}, \quad \text{(A10)}$$

$$D = \sqrt{B}\frac{V+\sqrt{B}\chi_h}{T_c(V+\chi_{tot})}. \quad \text{(A11)}$$

The symplectic eigenvalue $\lambda_5 = 1$.

Then, for the locally generated LO scheme, the covariance matrix of the final Gaussian state ρ_{AB}^G shared between Alice and Bob can be written as [8,39]

$$\gamma_{AB}^G = \begin{pmatrix} V_a\mathbb{I} & \mathbb{C}\sigma_Z \\ \mathbb{C}\sigma_Z & V_b\mathbb{I} \end{pmatrix}, \quad \text{(A12)}$$

where $\mathbb{I}$ is diag(1, 1), σ_Z is diag(1, -1), $V_a = V_A + 1$, $V_b = T_e(V+\chi)$, $\mathbb{C} = \overline{\cos\varphi}\sqrt{T_e(V_a^2-1)}$ for the locally generated LO scheme. Here $T_e = \eta_F\eta T$, χ is the channel noise and is equal to $(1-T_e)/T_e + v_{el}/T_e + \epsilon_0$. $\overline{\cos\varphi} = \int_{-\pi}^{\pi} d\varphi\mathcal{P}(\varphi)cos\varphi$ and $\mathcal{P}(\varphi)$ is the probability distribution of the phase estimation error φ. Therefore, I_{AB} can be written as

$$I_{AB} = \frac{1}{2}\log_2\left(\frac{V'}{V_{a|b}}\right) \quad \text{(A13)}$$

with $V' = (V_a+1)/2$ and $V_{a|b} = V' - \mathbb{C}^2/2V_b$. The Holevo bound χ_{BE} can be given by

$$\chi_{BE} = G\left(\frac{\lambda_1'-1}{2}\right) + G\left(\frac{\lambda_2'-1}{2}\right) - G\left(\frac{\lambda_3'-1}{2}\right). \quad \text{(A14)}$$

The eigenvalues λ_1' and λ_2' are given by

$$\lambda_{1,2}'^2 = \frac{1}{2}\left(\Delta \pm \sqrt{\Delta^2 - 4\mathbb{D}^2}\right) \quad \text{(A15)}$$

with $\Delta = V_a^2 + V_b^2 - 2\mathbb{C}^2$ and $\mathbb{D} = V_aV_b - \mathbb{C}^2$. The square of symplectic eigenvalue λ_3' reads:

$$\lambda_3'^2 = V_a(V_a - \frac{\mathbb{C}^2}{V_b}). \quad \text{(A16)}$$

Note, $\mathbb{C}^2$ can be written as [8,24]

$$\mathbb{C}^2 = T_e(V_a^2-1)\overline{cos\phi}^2 = T_e(V_a^2-1)(1-V_{\hat{\theta}}) \quad \text{(A17)}$$

with $V_{\hat{\theta}} = (\chi+1)/V_R + \delta_R/T_eV_R$, where $\delta_R = 1$ for single-reference-pulse mode, V_R is the amplitude of weak reference pulse.

References

1. Bennett, C.H.; Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In Proceedings of the IEEE International Conference on Computers Systems, and Signal Processing, Bangalore, India, 9–12 December 1984; pp. 175–179.
2. Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef] [PubMed]

3. García-Patrón, R.; Cerf, N.J. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503. [CrossRef] [PubMed]
4. Navascués, M.; Grosshans, F.; Acín, A. Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502. [CrossRef] [PubMed]
5. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **2010**, *81*, 062343. [CrossRef]
6. Furrer, F.; Franz, T.; Berta, M.; Leverrier, A.; Scholz, V.B.; Tomamichel, M.; Werner, R.F. Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks. *Phys. Rev. Lett.* **2012**, *109*, 100502. [CrossRef] [PubMed]
7. Leverrier, A. Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States. *Phys. Rev. Lett.* **2015**, *114*, 070501. [CrossRef] [PubMed]
8. Soh, D.B.S.; Brif, C.; Coles, P.J.; Lütkenhaus, N.; Camacho, R.M.; Urayama, J.; Sarovar, M. Self-Referenced Continuous-Variable Quantum Key Distribution Protocol. *Phys. Rev. X* **2015**, *5*, 041010. [CrossRef]
9. Qi, B.; Lougovski, P.; Pooser, R.; Grice, W.; Bobrek, M. Generating the Local Oscillator "Locally" in Continuous-Variable Quantum Key Distribution Based on Coherent Detection. *Phys. Rev. X* **2015**, *5*, 041009. [CrossRef]
10. Huang, D.; Huang, P.; Lin, D.; Wang, C.; Zeng, G. High-speed continuous-variable quantum key distribution without sending a local oscillator. *Opt. Lett.* **2015**, *40*, 3695–3698. [CrossRef] [PubMed]
11. Li, Z.; Zhang, Y.C.; Xu, F.; Peng, X.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **2014**, *89*, 052301. [CrossRef]
12. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Gui, M.; Liang, L.M. Gaussian-modulated coherent-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **2014**, *89*, 042335. [CrossRef]
13. Wu, Y.D.; Zhou, J.; Gong, X.B.; Guo, Y.; Zhang, Z.M.; He, G.Q. Continuous-variable measurement-device-independent multipartite quantum communication. *Phys. Rev. A* **2016**, *93*, 022325.10.1103/PhysRevA.93.022325. [CrossRef]
14. Huang, D.; Huang, P.; Lin, D.; Zeng, G. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* **2016**, *6*, 19201. [CrossRef] [PubMed]
15. Qu, Z.; Djordjevic, I.B.; Neifeld, M.A. RF-subcarrier-assisted four-state continuous-variable QKD based on coherent detection. *Opt. Lett.* **2016**, *41*, 5507–5510. [CrossRef] [PubMed]
16. Pirandola, S.; Ottaviani, C.; Spedalieri, G.; Weedbrook, C.; Braunstein, S.L.; Lloyd, S.; Gehring, T.; Jacobsen, C.S.; Andersen, U.L. High-rate measurement-device-independent quantum cryptography. *Nat. Photon.* **2015**, *9*, 397. [CrossRef]
17. Fossier, S.; Diamanti, E.; Debuisschert, T.; Tualle-Brouri, R.; Grangier, P. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. *J. Phys. B* **2009**, *42*, 114014. [CrossRef]
18. Huang, P.; He, G.; Fang, J.; Zeng, G. Performance improvement of continuous-variable quantum key distribution via photon subtraction. *Phys. Rev. A* **2013**, *87*, 012317. [CrossRef]
19. Li, Z.; Zhang, Y.; Wang, X.; Xu, B.; Peng, X.; Guo, H. Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution. *Phys. Rev. A* **2016**, *93*, 012310. [CrossRef]
20. Guo, Y.; Liao, Q.; Wang, Y.; Huang, D.; Huang, P.; Zeng, G. Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction. *Phys. Rev. A* **2017**, *95*, 032304.10.1103/physreva.95.032304. [CrossRef]
21. Liao, Q.; Guo, Y.; Huang, D.; Huang, P.; Zeng, G. Long-distance continuous-variable quantum key distribution using non-Gaussian state-discrimination detection. *New J. Phys.* **2018**, *20*, 023015. [CrossRef]
22. Guo, Y.; Li, R.; Liao, Q.; Zhou, J.; Huang, D. Performance improvement of eight-state continuous-variable quantum key distribution with an optical amplifier. *Phys. Lett. A* **2018**, *382*, 372–381. [CrossRef]
23. Wang, Y.J.; Wang, X.D.; Huang, D.; Guo, Y. Improving the Maximum Transmission Distance of Self-Referenced Continuous-Variable Quantum Key Distribution Using a Noiseless Linear Amplifier. *Entropy* **2018**, *20*, 461. [CrossRef]
24. Zhong, H.; Wang, Y.; Wang, X.; Liao, Q.; Wu, X.; Guo, Y. Enhancing of Self-Referenced Continuous-Variable Quantum Key Distribution with Virtual Photon Subtraction. *Entropy* **2018**, *20*, 578. [CrossRef]
25. Fang, J.; Huang, P.; Zeng, G. Multichannel parallel continuous-variable quantum key distribution with Gaussian modulation. *Phys. Rev. A* **2014**, *89*, 022315. [CrossRef]

26. Huang, D.; Lin, D.; Wang, C.; Liu, W.; Fang, S.; Peng, J.; Huang, P.; Zeng, G. Continuous-variable quantum key distribution with 1 Mbps secure key rate. *Opt. Express* **2015**, *23*, 17511–17519. [CrossRef] [PubMed]
27. Qu, Z.; Djordjevic, I.B. High-speed free-space optical continuous-variable quantum key distribution enabled by three-dimensional multiplexing. *Opt. Express* **2017**, *25*, 7919–7928.10.1364/oe.25.007919. [CrossRef] [PubMed]
28. Dynes, J.F.; Kindness, S.J.; Tam, S.W.B.; Plews, A.; Sharpe, A.W.; Lucamarini, M.; Fröhlich, B.; Yuan, Z.L.; Penty, R.V.; Shields, A.J. Quantum key distribution over multicore fiber. *Opt. Express* **2016**, *24*, 8081–8087. [CrossRef] [PubMed]
29. Bacco, D.; Ding, Y.; Dalgaard, K.; Rottwitt, K.; Oxenløwe, L.K. Space division multiplexing chip-to-chip quantum key distribution. *Sci. Rep.* **2017**, *7*, 12459.10.1038/s41598-017-12309-3. [CrossRef] [PubMed]
30. Ding, Y.; Bacco, D.; Dalgaard, K.; Cai, X.; Zhou, X.; Rottwitt, K.; Oxenløwe, L.K. High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. *NPJ Quantum Inf.* **2017**, *3*, 25. [CrossRef]
31. Hayashi, T.; Taru, T.; Shimakawa, O.; Sasaki, T.; Sasaoka, E. Design and fabrication of ultra-low crosstalk and low-loss multi-core fiber. *Opt. Express* **2011**, *19*, 16576–16592. [CrossRef] [PubMed]
32. Koshiba, M.; Saitoh, K.; Takenaga, K.; Matsuo, S. Analytical Expression of Average Power-Coupling Coefficients for Estimating Intercore Crosstalk in Multicore Fibers. *IEEE Photonics J.* **2012**, *4*, 1987–1995. [CrossRef]
33. Fujisawa, T.; Amma, Y.; Sasaki, Y.; Matsuo, S.; Aikawa, K.; Saitoh, K.; Koshiba, M. Crosstalk Analysis of Heterogeneous Multicore Fibers Using Coupled-Mode Theory. *IEEE Photonics J.* **2017**, *9*, 1–8. [CrossRef]
34. Qi, B.; Huang, L.L.; Qian, L.; Lo, H.K. Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Phys. Rev. A* **2007**, *76*, 052323. [CrossRef]
35. Kumar, R.; Qin, H.; Alléaume, R. Coexistence of continuous variable QKD with intense DWDM classical channels. *New J. Phys.* **2015**, *17*, 043027. [CrossRef]
36. Patel, K.A.; Dynes, J.F.; Lucamarini, M.; Choi, I.; Sharpe, A.W.; Yuan, Z.L.; Penty, R.V.; Shields, A.J. Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks. *Appl. Phys. Lett.* **2014**, *104*, 051123. [CrossRef]
37. Qi, B.; Zhu, W.; Qian, L.; Lo, H.K. Feasibility of quantum key distribution through a dense wavelength division multiplexing network. *New J. Phys.* **2010**, *12*, 103042. [CrossRef]
38. Pirandola, S.; Mancini, S.; Lloyd, S.; Braunstein, S.L. Continuous Variable Quantum Cryptography using Two-Way Quantum Communication. *Nat. Phys.* **2006**, *4*, 726–730. [CrossRef]
39. García-Patrón Sánchez, R.; Cerf, N. Quantum Information With Optical Continuous Variables: From Bell Tests to Key Distribution. Available online: http://difusion.ulb.ac.be/vufind/Record/ULB-DIPOT:oai:dipot.ulb.ac.be:2013/210655/TOC (accessed on 12 October 2007).