mathematics

MDPI

Article

Adaptive Continuous-Variable Quantum Key Distribution with Discrete Modulation Regulative in Free Space

Yiwu Zhu [1], Lei Mao [1], Hui Hu [1], Yijun Wang [1,*] and Ying Guo [1,2,*]

[1] School of Automation, Central South University, Changsha 410083, China
[2] School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China
* Correspondence: xxywyj@sina.com.cn (Y.W.); guoying@bupt.edu.cn (Y.G.)

Abstract: The finite sampling bandwidth of an analog-to-digital converter has a negative effect on the continuous-variable quantum key distribution (CVQKD), which leaves a potential loophole for an eavesdropper and weakens the practical security of the system. To compensate for the loss in free space, we deploy an adaptive optics (AO) unit in the detector of the CVQKD system with discrete modulations. Since the closed-loop control bandwidth of the embedded AO unit can be optimized with the sampling frequency, the practical security of the system can be enhanced in terms of the secret key rate. The security analysis is demonstrated on the basis of the derived secret key rate with numerical simulations, providing a feasible implementation of CVQKD in realistic free-space environments.

Keywords: quantum key distribution; free space; continuous-variable; quantum communications; quantum cryptography

MSC: 81P94; 81P45

Citation: Zhu, Y.; Mao, L.; Hu, H.; Wang, Y.; Guo, Y. Adaptive Continuous-Variable Quantum Key Distribution with Discrete Modulation Regulative in Free Space. *Mathematics* **2022**, *10*, 4450. https://doi.org/10.3390/math10234450

Academic Editor: Jonathan Blackledge

Received: 18 October 2022
Accepted: 21 November 2022
Published: 25 November 2022

1. Introduction

Quantum key distribution (QKD) [1–4], which randomly generates secret keys for legal participants, can be composed of discrete-variable (DV) QKD [1,2] and continuous-variable (CV) QKD [3,4]. The former encodes information of key bits in the polarization states of a single photon, whereas the latter encodes information with the momentum and position quadratures ($\hat{x}$ and $\hat{p}$) of an optical field that involves Gaussian modulation. The security has been proven in both finite-size regimes and asymptotic limits [5]. The traditional CVQKD can be implemented with Gaussian modulations (GM). However, it is difficult to break the limitation of a low signal-to-noise ratio (SNR), which results in a decline in reconciliation efficiency. As a result, a discretely modulated (DM) CVQKD has been proposed to address such limitations and the security has been demonstrated in the asymptotic regime [6]. Unfortunately, it is still vulnerable to insecure loopholes, which have an effect on practical security when performing potential attack strategies, such as local oscillator (LO) fluctuation attacks [7], LO calibration attacks [8], wavelength attacks [9], saturation attacks [10], finite sampling bandwidth effects [11], blinding attacks on the detector [12], jitter in clock synchronization [13], polarization attacks [14], side-channel attacks [15,16], and so on. In consequence, a large number of countermeasures have been proposed [17]. A measurement-device-measurement (MDI) scheme has been used for defending attacks in detectors [18,19]. However, it remains vulnerable because of imperfect equipment that contains concealed loopholes in practical systems.

When being implemented in free-space (FS) channels, the transmission coefficient fluctuates because of turbulent atmospheric effects. As coherent detection can be distorted by atmospheric turbulence, the performance of the system will be degraded. Fortunately, suitable adaptive optics (AO) can be used to mitigate turbulence-induced wavefront aberrations of the received quantum states. In this paper, we demonstrate the effects of a

finite sampling bandwidth on the practical security of CVQKD regulative in free space. An AO-enabled approach is used for performance improvement in terms of the secret key rate.

This paper is organized as follows: In Section 2, we propose an AO-embedded detector for a free-space CVQKD system with discrete modulations. In Section 3, we demonstrate the effect of the finite sampling bandwidth on the practical security of the AO-enabled CVQKD system when considering collective attacks. We evaluate the secret key rate with numerical simulations using a linear model by taking the effects of the finite sampling bandwidth into account. Finally, conclusions are drawn in Section 4.

2. AO-Enabled CVQKD with Discrete Modulations

In the prepare-and-measure scheme, there are usually N coherent states denoted as $|\alpha_k^N\rangle = |\alpha e^{i2k\pi/N}\rangle$ with modulation variance $V_M = 2\alpha^2$ for $k \in Z_N = \{0, 1, \cdots, N-1\}$ [20]. Each coherent state $|\alpha_k^N\rangle$ can be represented using the amplitude quadrature ($\hat{x}$) and the phase quadrature ($\hat{x}$). Alice prepares N coherent states and sends one of the coherent states at random to the receiver Bob in free space, which can be characterized using the transmission T and the excess noise ϵ. Upon receiving the coherent states, Bob performs either a homodyne detector or a heterodyne detector to measure one of the two quadratures $\hat{x}$ or $\hat{p}$ or both the quadratures.

To simplify the description of the proposed CVQKD system, we consider an equivalent entanglement-based scheme with discrete modulations. As shown in Figure 1, Alice prepares for N coherent states given by

$$|\Psi_N\rangle = \frac{1}{4}\sum_{k=0}^{N-1} |\psi_k\rangle|\beta_k\rangle, \tag{1}$$

where the states $|\psi_k\rangle$ for $k \in Z_N$ can be described as

$$|\psi_k\rangle = \frac{1}{2}\sum_{m=0}^{N-1} e^{i(\frac{N}{2}k+1)m\pi/4}|\phi_k\rangle. \tag{2}$$

Moreover, the state $|\phi_k\rangle$ for $k \in Z_N$ can be described as

$$|\phi_k\rangle = \frac{e^{-\frac{\alpha^2}{2}}}{\sqrt{\lambda_k}}\sum_{n=0}^{\infty}(-1)^n e^{\frac{\alpha(Nn+k)}{\sqrt{(Nn+k)!}}}|(Nn+k)\rangle. \tag{3}$$

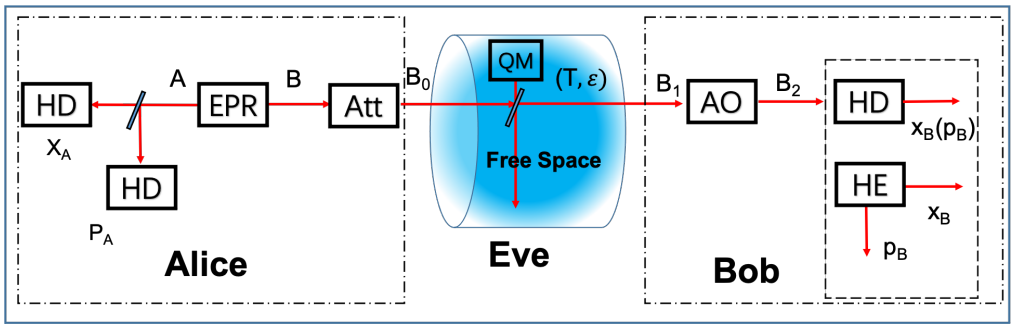

Figure 1. Scheme diagram of the AO-enabled CVQKD with discrete modulations. HD and HE denote homodyne detection or heterodyne detection, Att denotes attenuation, QM denotes quantum memory, and EPR is a two-mode squeezed vacuum (EPR) state.

In Figure 1, we present a schematic diagram of the AO-based DM CVQKD in free space. Alice prepares for the bipartite state $|\Psi_N\rangle$, as described in Equation (1), with modulation variance $V = 1 + V_M$. She measures the coherent states projected on mode A, while projecting another state to mode B that is transmitted in free space. Afterwards, Bob can

perform either homodyne detection (HD) or heterodyne detection (HE) to measure the received mode B_2.

At the receiver, we consider the influence of the finite sampling bandwidth on the estimated secret key rate of the CVQKD system. The AO-embedded detector can realize the real-time detection of a distorted wavefront and then correct the distorted wavefront, which can be used for potential loss compensation in free space.

2.1. Finite Sampling Frequency

As is well-known in traditional optical signal processing, frequency aliasing usually leads to the distinct spectrum of discrete Fourier transformation (DFT), and, thus, an analog-to-digital converter with decreased finite sampling frequency will fail to restore the initial signals at the receiver. Taking into account $f_s \in \{50, 100, 200\}$ Hz as an example, the spectrum may overlap with the decreasing sampling frequency. According to the optical signal processing, we can find the signal distortion, though the restored signal shapes can be produced like a Gaussian-distribution sampled at the above-mentioned frequency f_s.

While performing the DFT operation, we find that the low sampling frequency leads to frequency aliasing in the frequency domain. With increasing sampling frequency, the restored signals approach the original Gaussian-distribution signals. The reason is that fewer sampling points may result in unavoidable information loss in terms of signal-restored processing. Only when the sampling frequency is twice the signal frequency can the sample value approach the maximal value of the output signals. Therefore, we focus on the influence of the finite sampling frequency in the frequency domain. To offset the loophole, a suitable sampling frequency for state preparation is recommended for attenuation (Att), resulting in less electrical noise.

2.2. AO-Embedded Detector

As shown in Figure 1, an AO unit, which includes a wavefront corrector, a wavefront controller and a wavefront sensor, can be embedded in the detector to compensate for the loss in free space. The AO-embedded detector can be used for performance improvement of the CVQKD system in free space.

When Bob performs optical coherent detection to estimate the excess noise, he needs a combination of the received optical signals and other signals derived from local oscillation (LO). We assume that the LO laser turns to plane waves and the intensity of the optical signal passing through the AO unit is uniform. The efficiency introduced by the AO unit outweighs the AO-added noise. The total noise that includes the channel-added, the AO-added and the detection-added noise decreases due to the effect of the AO unit on the detector. Since the AO unit achieves real-time detection of the distorted wavefront and then controls it immediately, the quality of the transformed optical signal is improved [21,22].

3. Security Analysis

3.1. Derivation of the Secret Key Rate

Since CVQKD can be implemented with a pulsed signal light, the received signals, which can be described as the secret bit rate $R = f_s K$, depend on the sampling repetition rate f_s and the secret key rate K, thereby contributing to performance improvement. The secret key rate is an important parameter that can be used to assess the performance of the proposed system. To obtain the secret key rate, the covariance matrix should be derived. The secret key rate, in the case of an asymptotic framework, can be given by

$$K = \beta I_{AB} - \chi_{BE}, \tag{4}$$

where β is the reconciliation efficiency, I_{AB} refers to the mutual information shared by both Alice and Bob, and χ_{BE} represents the Holevo bound between Bob and Eve.

In what follows, the secret key rate is determined based on the reverse reconciliation ($\chi_E = \chi_{BE}$), where the Holevo bound χ_{BE} can be calculated as follows,

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

where $G(x) = (x+1)\log(x+1) - x\log(x)$. Taking the notation $T_{nf} = \langle T^2 \rangle$, the symplectic eigenvalues $\lambda_{1,2}$ can be described as

$$\lambda_{1,2}^2 = \frac{1}{2}[A \pm \sqrt{A^2 - 4B}] \tag{6}$$

with the denotations

$$\begin{aligned} A &= V^2(1-2T) + 2tT_{nf}T^2(V + \chi_{line})^2, \\ B &= T_{nf}^2(V\chi_{line} + 1)^2. \end{aligned} \tag{7}$$

The remaining symplectic eigenvalues $\lambda_{3,4,5}$ of the covariance matrix are calculated based on the above elements. Therefore, the eigenvalues $\lambda_{3,4}$ can be rewritten as

$$\lambda_{3,4}^2 = \frac{1}{2}[C + \sqrt{C^2 - 4D}], \tag{8}$$

where

$$\begin{aligned} C &= \frac{A(\chi_w + \chi_h) + V\sqrt{B} + T_{nf}(V + \chi_{line})}{T_{nf}(V + \chi_{tot})}, \\ D &= \frac{\sqrt{B} + B(\chi_w + \chi_h)}{T_{nf}(V + \chi_{tot})}, \end{aligned} \tag{9}$$

where $\chi_{tot} = \chi_{line} + (\chi_w + \chi_h)/T_{nf}$ is the total noise, and χ_{line} is the total channel-added noise introduced by atmospheric turbulence given by

$$\chi_{line} = V_T(V - 1 + \xi) + \langle T^2 \rangle^{-1} - 1, \tag{10}$$

with notation $V_T = \langle T \rangle - \langle \sqrt{T} \rangle^2$. In addition, the symplectic eigenvalue is $\lambda_5 = 1$. Let $\xi_{nf} = V_T(V - 1 + \xi)$, and then the above-derived noise can be rewritten as $\chi_{line} = 1/T_{nf} - 1 + \xi_{nf}$, which is characterized by the parameter transmission (T). Then the mutual information I_{AB} can be achieved as follows,

$$I_{AB} = \frac{1}{2}\log(\frac{V_A}{V_{A|B}}) = \frac{1}{2}\log(\frac{V + \chi_{tot}}{1 + \chi_{tot}}), \tag{11}$$

where χ_w is the AO-added noise, and χ_h is the detection-added noise. In this way, the secret key rate, which is based on the covariance matrix in the asymptotic framework, can be obtained.

3.2. Tunable Parameter Optimization

To optimize the performance of the system, we take into account the modulation variance V_M for coherence state preparation. According to the derived secret key rate K in Equation (5), this depends on the parameter of modulation variance V_M in the source preparation. Numerical simulations demonstrate the optimal interval where the minimal secret key rate is bound to be over 10^{-6} for the given maximal transmission distance $d \in \{60\text{ km}, 80\text{ km}, 100\text{ km}\}$, as shown in Figure 2, where the different transmission distances are represented with lines using respective colors. We find that the increasing transmission distance narrows down this interval $[0.02, 0.16]$. In the meantime, there is a

decline in the secret key rate. Narrow though each optimal interval is, every curve involves the common optimal interval, where the secret key rate reaches a peak for $V_M = 0.1$. As a result, we have an optimal modulation variance $V_M = 0.1$ in CVQKD according to the numerical simulations of the secret key rate for the variable modulated variance V_M in the range $[0, 0.2]$.

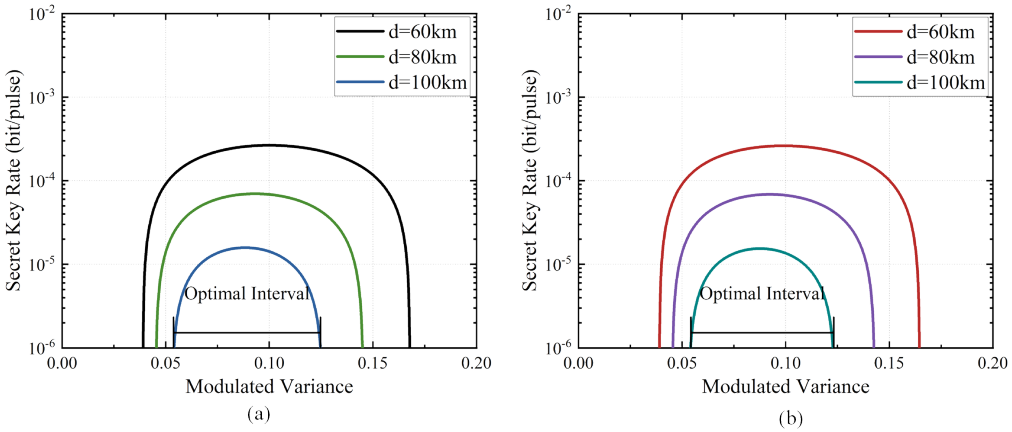

Figure 2. The secret key rate as a function of the modulated variance V_M for the given transmission distance $d \in \{60, 80, 100\}$ km of (**a**) eight-state DM DVQKD and (**b**) four-state DM CVQKD.

The sampling frequency also plays a role in the performance improvement, as shown in Figure 3, where the different frequencies $f_s \in \{2\text{ GHz}, 4\text{ GHz}, \infty\text{ GHz}\}$ are represented with lines using respective colors. We find that the increasing sampling frequency narrows down this interval $[0.01, 0.19]$. For the given variance V_M, the large sampling frequency results in an increased secret key rate. Similar to the above analysis, there is also a decline in the secret key rate for the modulated variance $V_M \in [0, 0.2]$. Moreover, as the sampling frequency reaches 4 GHz, the secret key rate approaches the optimal value. Consequently, we can select the values $f_s = 4$ GHz and $V_M = 0.1$ in numerical simulations.

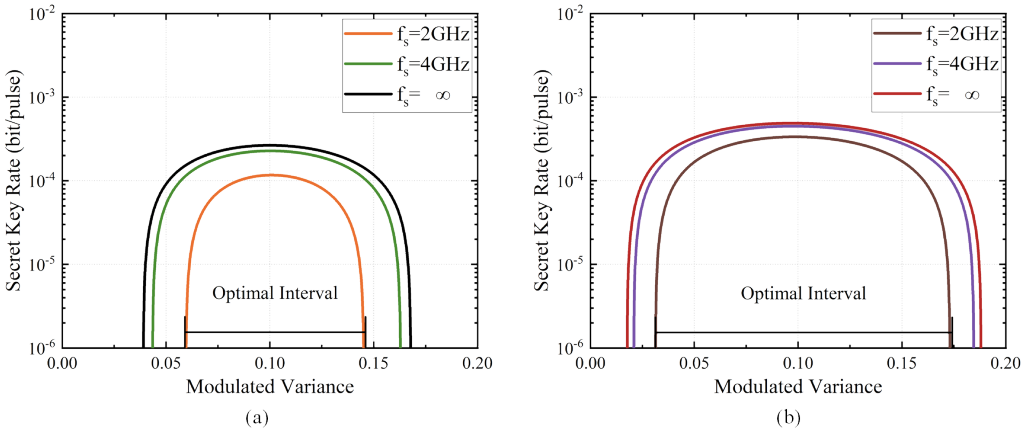

Figure 3. The secret key rate as a function of the modulated variance with sampling frequency $f_s \in \{2, 4, \infty\}$ GHz of (**a**) eight-state DM DVQKD and (**b**) four-state DM DVQKD.

3.3. Simulation Results

In Figure 4, we demonstrate the secret key rate of the AO-enabled DM CVQKD system for both (a) the four-state scheme and (b) the eight-state scheme, which is a function of the transmission ($T \in [0, 1]$), while illustrating the effect of the sampling frequency f_s on performance. In numerical simulations, we achieve a secret key rate for the given sampling frequency $f_s \in \{1\text{ GHz}, 2\text{ GHz}, 4\text{ GHz}, \infty\text{ GHz}\}$. The higher sampling frequency results in a higher secret key rate. It is observed that there is a decline in the secret key rate with

decreasing sampling frequency. The high-rate sampling frequency generates a high-rate CVQKD system due to the effect of the AO unit on the detector of the receiver, which can be regarded as compensation for the suffering it has been caused. Since the previously mentioned loophole can be solved at the AO-involved receiver, the eavesdropper has no access to the unsolved loophole. Given the finite sampling frequencies of ADC, for example $f_s = 4$ GHz, it can be used to apply a suitable ADC to achieve a practical high-rate CVQKD system.

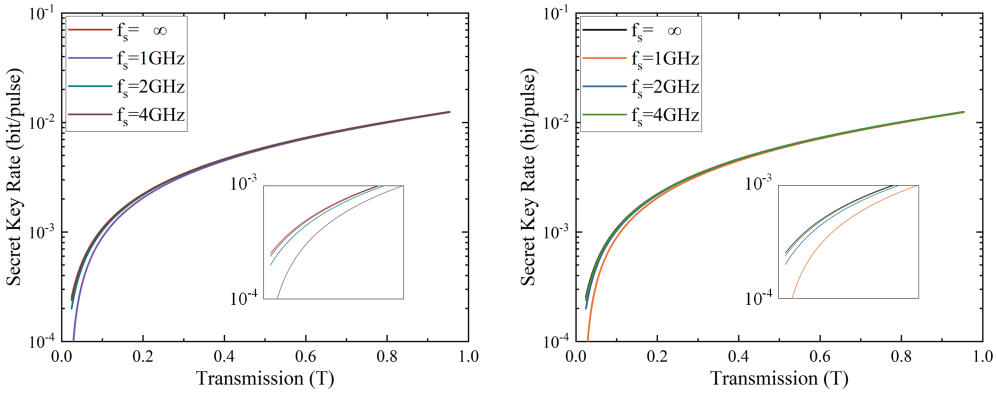

Figure 4. lThe secret key rate of the DM CVQKD system as a function of the transmission with $f_s \in \{1, 2, 4, \infty\}$ GHz by applying homodyne detection of (**a**) a four-state scheme and (**b**) an eight-state scheme. The lines from the top down denote the secret key rates of the system with frequencies ∞ GHz, 4 GHz, 2 GHz and 1 GHz, respectively. The higher sampling frequency means a higher secret key rate.

In Figure 5, we compare the secret key rate of the AO-enabled DM CVQKD system with the traditional system without embedding the AO unit, where the lines from the top down denote the secret key rates of the AO-enabled system and the traditional system, while considering the four-state scheme for modulations. We observe that the embedded AO unit in the receiver improves the performance of the system. Combined with Figure 4, the eight-state scheme performs only a little better than the four-state scheme in terms of the secret key rate when considering the effects of the AO unit on the secret key rate. However, as for the DM scheme for modulations, the AO unit cannot always be more advantaged compared with the traditional CVQKD system with Gaussian modulation.

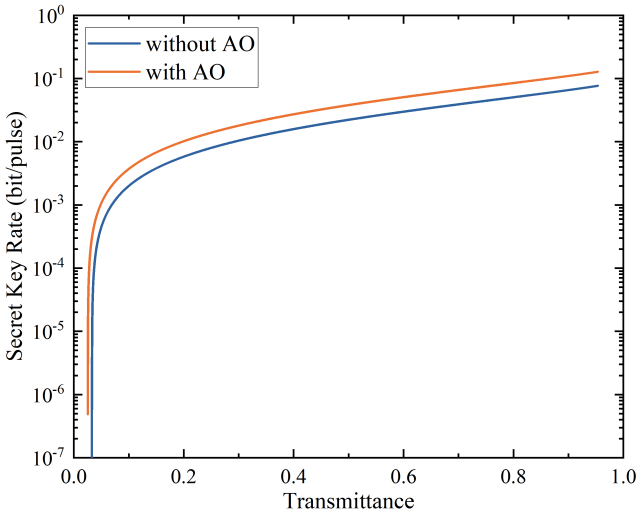

Figure 5. The performance of the AO-enabled DM CVQKD system for the four-state scheme.

4. Conclusions

We have proposed an AO-enabled DM CVQKD over an atmospheric turbulent channel and demonstrated the influence of the finite sampling frequency on performance improvement. We found that an increased sampling frequency may have a positive effect on performance. We illustrated the performance of the AO-enabled DM CVQKD over an atmospheric turbulent channel in the asymptotic regime, which resulted in an increased secret key rate. The proposal represents an elegant approach to performance improvement of a practical CVQKD system in FS-involved environments. With respect to other approaches to performance improvement, we can make use of non-Gaussian operations for source preparation or signal detection, which will be investigated in future work.

Author Contributions: Conceptualization, Y.Z.; writing—original draft preparation, L.M.; writing—review, Y.W. and H.H.; writing—editing, Y.G. All authors have read and agree to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (Grant No. 61871407), and the Special Funds for the Construction of an Innovative Province in Hunan (Grant No. 2022GK2016).

Data Availability Statement: All data generated or analyzed during this study are included in this published article.

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

References

1. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
2. Scarani, V.; Renner, R. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.* **2008**, *100*, 200501. [CrossRef] [PubMed]
3. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef] [PubMed]
4. Grosshans, F.; Van Assche, G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241. [CrossRef]
5. Guo, Y.; Liao, Q.; Huang, D.; Zeng, G. Quantum relay schemes for continuous-variable quantum key distribution. *Phys. Rev. A* **2017**, *95*, 042326. [CrossRef]
6. Leverrier, A.; Grangier, P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.* **2008**, *102*, 180504. [CrossRef]
7. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A* **2013**, *87*, 062313. [CrossRef]
8. Huang, J.Z.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Li, H.W.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A* **2013**, *87*, 062329. [CrossRef]
9. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Liang, L.M. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. *Phys. Rev. A* **2013**, *87*, 052309. [CrossRef]
10. Qin, H.; Kumar, R. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Phys. Rev. A* **2016**, *94*, 012325. [CrossRef]
11. Wang, C.; Huang, P.; Huang, D.; Lin, D.; Zeng, G. Practical security of continuous-variable quantum key distribution with finite sampling bandwidth effects. *Phys. Rev. A* **2016**, *93*, 022315. [CrossRef]
12. Qin, H.; Kumar, R.; Makarov, V. Homodyne-detector-blinding attack in continuous-variable quantum key distribution. *Phys. Rev. A* **2018**, *98*, 012312. [CrossRef]
13. Guo, Y.; Xie, C.; Liao, Q. Entanglement-distillation attack on continuous-variable quantum key distribution in a turbulent atmospheric channel. *Phys. Rev. A* **2017**, *96*, 022320. [CrossRef]
14. Guo, Y.; Ye, W.; Zhong, H.; Liao, Q. Continuous-variable quantum key distribution with non-Gaussian quantum catalysis. *Phys. Rev. A* **2019**, *99*, 032327. [CrossRef]
15. Schneider, T.; Moradi, A.; Güneysu, T. ParTI-Towards Combined Hardware Countermeasures Against Side-Channel and Fault-Injection Attacks. In Proceedings of the 36th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO 2016), Santa Barbara, CA, USA, 14–18 August 2016 ; Volume 9815, pp. 302–332.
16. Dofe, J.; Pahlevanzadeh, H.; Yu, Q. A Comprehensive FPGA-Based Assessment on Fault-Resistant AES against Correlation Power Analysis Attack. *J. Electron. Test.* **2016**, *32*, 611–624. [CrossRef]
17. Kunz-Jacques, S.; Jouguet, P. Robust shot-noise measurement for continuous-variable quantum key distribution. *Phys. Rev. A* **2015**, *91*, 022307. [CrossRef]

18. Pir, ola, 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. Photonics* **2015**, *9*, 397–402.
19. 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]
20. Liao, Q.; Xiao, G.; Xu, C.; Xu, Y.; Guo, Y. Discretely-modulated continuous-variable quantum key distribution with untrusted entanglement source. *Phys. Rev. A* **2020**, *102*, 032604. [CrossRef]
21. Huang, J.; Deng, K.; Liu, C.; Zhang, P.; Jiang, D.; Yao, Z. Effectiveness of adaptive optics system in satellite-to-ground coherent optical communication. *Opt. Express* **2014**, *22*, 16000–16007.
22. Liu, W.; Yao, K.; Huang, D.; Lin, X.; Wang, L.; Lv, Y. Performance evaluation of coherent free space optical communications with a double-stage fast-steering-mirror adaptive optics system depending on the Greenwood frequency. *Opt. Express* **2016**, *24*, 13288–13302. [CrossRef] [PubMed]