entropy

MDPI

Review

Geometrical Optics Restricted Eavesdropping Analysis of Satellite-to-Satellite Secret Key Distillation

Ziwen Pan * and Ivan B. Djordjevic

Department of Electrical & Computer Engineering, College of Engineering, The University of Arizona, 1230 E Speedway Blvd, Tucson, AZ 85721, USA; ivan@arizona.edu
* Correspondence: ziwenpan@email.arizona.edu

Abstract: Traditionally, the study of quantum key distribution (QKD) assumes an omnipotent eavesdropper that is only limited by the laws of physics. However, this is not the case for specific application scenarios such as the QKD over a free-space link. In this invited paper, we introduce the geometrical optics restricted eavesdropping model for secret key distillation security analysis and apply to a few scenarios common in satellite-to-satellite applications.

Keywords: geometrical optics restricted eavesdropping; secret key distillation; satellite-to-satellite

Citation: Pan, Z.; Djordjevic, I.B. Geometrical Optics Restricted Eavesdropping Analysis of Satellite-to-Satellite Secret Key Distillation. *Entropy* **2021**, *23*, 950. https://doi.org/10.3390/e23080950

Academic Editor: Jay Lawrence

Received: 14 June 2021
Accepted: 21 July 2021
Published: 25 July 2021

1. Introduction

Quantum key distribution is known to guarantee unconditional security. The first QKD protocol, BB84, was developed in 1984 [1], which uses the polarization states of single photons to safely distribute keys. This was also known as the first discrete variable (DV)-QKD. Different protocols have since been studied, such as device-independent protocols that study the security with compromised apparatus [2–5], high dimensional protocols that exploit high dimensional degrees of freedom to increase the key rate [6–10] and decoy state protocols [11–13] that use decoy states against the photon-number-splitting attack [14]. Another major category in the study of QKD protocols, the continuous variable (CV) protocols [15,16] that encode keys into CV observables of carrier fields [17], are known to be more easily implementable for their compatibility with current communication devices instead of relying on single-photon generation and detection like most DV protocols.

Generally, in this paper, we assume that Alice uses a multi-photon source governed by the mean photon number without photon-number-resolving detectors so that she is limited in knowing whether she is transmitting a multi-photon wave packet, for example, if she only has a Geiger mode detector that clicks when one or more photons are detected. For security analysis of the quantum key distribution under these assumptions, conventionally, an omnipotent eavesdropper (Eve) that can gather information from the multi-photon wave packets transmitted from Alice to Bob by collecting every photon that does not arrive at Bob's receiver is assumed [18–25]. However, this is not the case for some specific application scenarios. For example, it would be reasonable to assume that the eavesdropper's (Eve's) power collection ability is limited due to the size of her aperture in an optical wireless channel from Alice to Bob. In [26,27], geometrical optics restricted eavesdropping analysis was proposed, considering the reasonably limited power collection ability of Eve. In [28–33], some of the applications of this restricted Eve model were introduced.

In this invited paper, we present some of the applications of the geometrical optics restricted model. In Section 2, we briefly introduce the power-collection-restricted eavesdropping model and give the lower and upper bound expressions. In Section 3.1, we showcase geometrical optics restricted eavesdropping analysis with a case where the eavesdropper has an aperture of a limited size in the same plane as Bob's while investigating the exclusion zone as one of Bob's defense strategies. In Section 3.2, we further assume that Eve's aperture can be dynamically positioned and provide the results while optimizing this

eavesdropping strategy. We conclude that the geometrical optics restricted eavesdropping model is suitable for multiple application scenario analysis.

2. Geometrical Optics Restricted Eavesdropping Model

As is illustrated in Figure 1, instead of assuming that Eve collects all the photons outside of Bob's receiver, only a fraction κ of them is collectable by Eve, denoted here as a wiretap channel with a κ-transmissivity beamsplitter. Here, η is the Alice-to-Bob channel transmissivity, μ is the input mean photon number per mode on Alice's side, and n_e is the noise mean photon number per mode on Eve's side. $\psi^{AA'}$ and $\psi^{EE'}$ in Figure 1 are entanglement pairs. Alice would keep mode A and send mode A' to Bob, and in the most general case, Eve would also use entanglement pairs to eavesdrop, retaining mode E and sending mode E' into the channel. In [26], the lower bound on the achievable key rate for direct and reverse reconciliation is shown below:

$$K_{\rightarrow} \geq \beta g(n_e(1-\eta)+\eta\mu) - \sum_i g\left(\frac{\nu_{y_i}^{ER}-1}{2}\right) - \beta g(n_e(1-\eta)) + g(n_e(1-\eta\kappa)), \quad (1)$$

$$K_{\leftarrow} \geq \beta g(\mu) - \sum_i g\left(\frac{\nu_{y_i}^{ER}-1}{2}\right) - \beta g\left(\mu - \frac{\eta\mu(1+\mu)}{1+n_e-n_e\eta+\eta\mu}\right) + \sum_i g\left(\frac{\nu_{y_i}^{ER}-1}{2}\right), \quad (2)$$

$$g(x) = (x+1)\log_2(x+1) - x\log_2 x \quad (3)$$

with detailed expressions of $\nu_{y_i}^{ER}$ available in [26]. Here, β is the reconciliation efficiency, which is set to $\beta = 1$ throughout this paper.

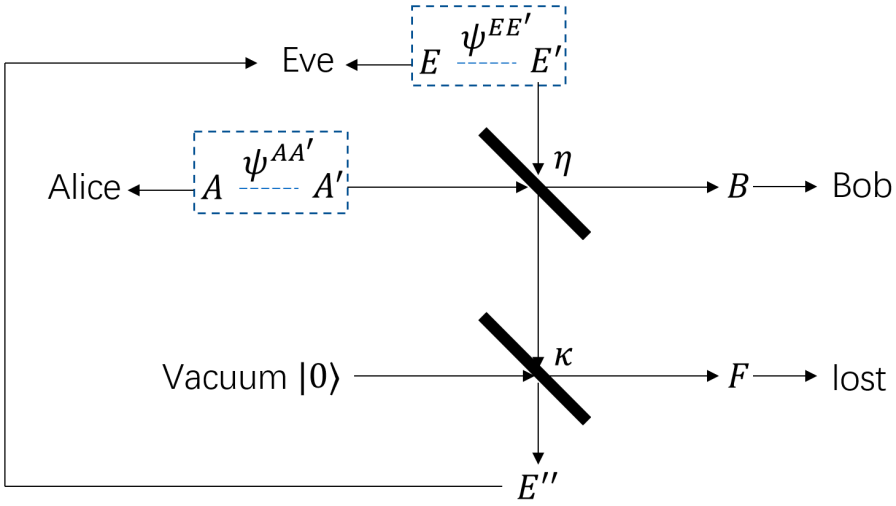

Figure 1. Geometrical optics restricted model wiretap channel notation [26].

The upper bound in a pure loss channel ($n_e = 0$) is shown to be [26]

$$K \leq \log_2 \frac{\eta + \kappa(1-\eta)}{\kappa(1-\eta)}, \quad (4)$$

while the upper bound in a thermal noise channel does not have a closed form expression. Detailed calculations can be found in Appendix A of [26].

3. Applications on Satellite-to-Satellite Secret Key Distillation

In this section, we study some applications of the geometrical optics restricted model analysis that would be common in satellite-to-satellite links where Eve's collecting ability would be naturally limited due to the radius of her receiver aperture, which usually ranges from centimeters to decimeters for traditional free-space communication. If we take existing

space applications into account for an upper-bounding estimation of Eve's aperture size, the Giant Magellan Telescope, one of the largest optical observatories, has a primary mirror of a 12.5-m radius [34]. Other known aperture sizes of satellite-based applications are much smaller, such as the 1.2-m-radius primary mirror for the Hubble Space Telescope [35] and the 20-cm-radius aperture for NASA's "Wide-field Infrared Survey Explorer" infrared telescope [36].

We analyze both the communication parties' and Eve's strategy by starting with a defense strategy from Bob's side called an exclusion zone, under the aforementioned assumptions and considering the case where Eve's aperture is in the same plane with Bob's in Section 3.1. Then, in Section 3.2, we move forward from that and assume that Eve's aperture can be dynamically positioned, concluding Eve's strategy for eavesdropping. In this section, we assume that a Gaussian beam with a beam waist W_0 and wavelength $\lambda = 1550$ nm is transmitted. The space temperature is set to $T = 3$ K, and we calculate the noise mean photon number using the black body radiation equation:

$$n_e = \frac{1}{e^{\frac{hf}{kT}} - 1}, \tag{5}$$

where h is the Planck constant, f is the transmission center frequency, and k is the Boltzmann constant. We then calculate the power transmitted by Alice P_{Alice}, the power received by Bob P_{Bob}, the power received by Eve P_{Eve}, and the channel transmissivity η, and the restriction factor on Eve κ can be expressed as

$$\eta = \frac{P_{Bob}}{P_{Alice}}, \tag{6}$$

$$\kappa = \frac{P_{Eve}}{P_{total}(1-\eta)}, \tag{7}$$

In this section, we calculate the lower bound as the maximum of the direct reconciliation lower bound and the reverse reconciliation lower bound.

3.1. Bob's Defense Strategy: Exclusion Zone

In this subsection, we introduce the problem set-up of one of the most straightforward defense strategies of the communication parities: the so-called exclusion zone. In principle, the closer Eve is to the beam transmission axis from Alice to Bob, the more likely the legitimate communication parities would detect the eavesdropper's presence (e.g., with a naïve approach such as a visible or infrared telescope or even radar to detect the eavesdropper's presence and abort communication if a possible eavesdropper is detected within a certain range to the communication parities). In free-space channels such as the satellite links, it is also possible for Bob to have opaque material around his receiver to absorb any photons that might have arrived outside of his receiver's aperture, preventing them from further propagation and possibly ending up in Eve's receiver aperture. As is illustrated in Figure 2, the exclusion zone is denoted with a dashed circle around Bob's receiver, excluding potential eavesdroppers to collect photons that arrive in this region. By definition, Bob's aperture area is also part of the exclusion zone, since the photons arriving at Bob's aperture would not be collectable by Eve. Here, more specifically, we say that Bob is setting up an exclusion zone if the area of the exclusion zone (A_{ex}) is larger than his receiver aperture area (A_{Bob} or A_b). Other specified parameters include L being the transmission distance and A_{Alice} (A_a) and A_{Eve} (A_e) being the area of Alice's aperture (radius r_a) and Eve's aperture (radius r_e), respectively. The radii of Bob's aperture and the exclusion zone are denoted as r_b and r_{ex} ($r_{ex} \geq r_b$). Here, the limited size of Eve's aperture is placed in the same plane as Bob's, since that would be the worst-case scenario for the purpose of our study under this exclusion zone assumption if Eve is not allowed between the Alice-to-Bob line of sight.

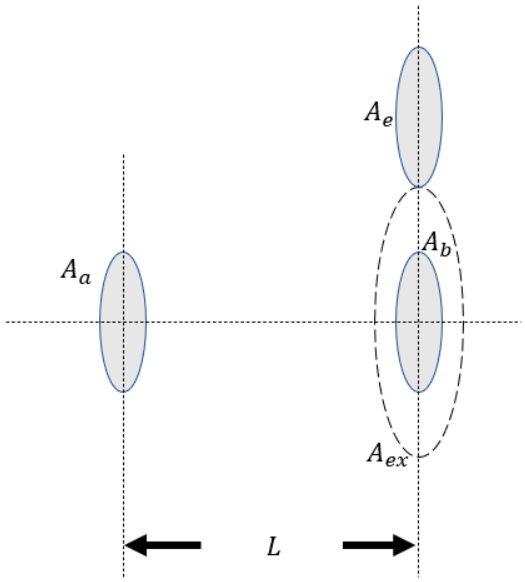

Figure 2. Limited size aperture of Eve in the same plane as Bob's. Here, Bob is setting an exclusion zone around his receiver as a defense strategy.

To start with, we set $r_{ex} = r_b$ (no additional exclusion zone) and investigate how Eve's aperture size would affect the achievable secure key rate lower bound (LB) and upper bound (UB), as shown in Figure 3. Here, we can see that under these parameters, the lower bound was quite close to the upper bound, which gave us the capacity in this scenario. As Eve's aperture size increased, the achievable rate went down and saturated but still outperformed the unrestricted case capacity. The reason for this convergence is that the transmitted beam intensity was the strongest at its center and weakened fast in the outer regions. As such, up to some point, increasing Eve's aperture size would only be able to gather photons from the regions far away from the beam center, thus making it ineffective in increasing Eve's advantage. As a result of that, in the figure below, we only set Eve's aperture radius to be 10 cm, equal to r_a and r_b, for a fair comparison.

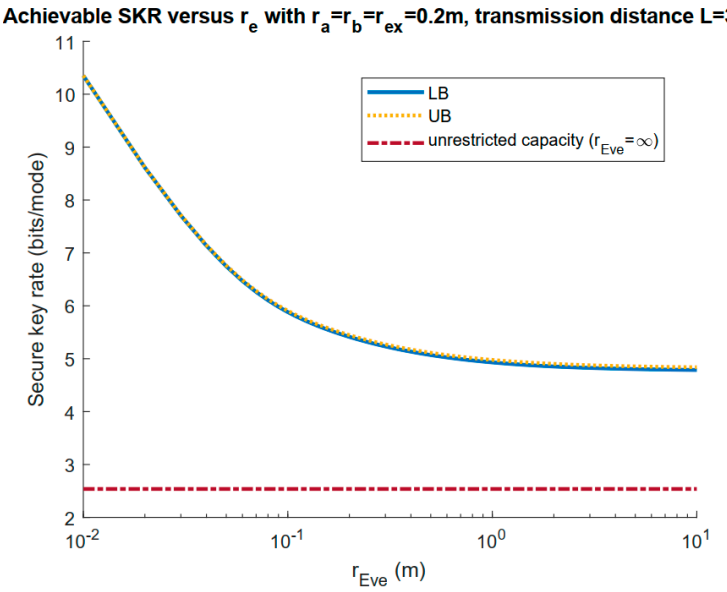

Figure 3. Achievable secure key rate lower and upper bound as functions of Eve's aperture radius r_e, with $r_{ex} = r_b$. The unrestricted case (infinite-sized aperture on Eve's side) is also included. Here, $W_0 = r_a = r_b = r_{ex} = 20$ cm.

In Figure 4, we set the exclusion zone radius to be $r_{ex} = 15$ cm and 20 cm to compare the achievable rate lower bounds (LB) and upper bounds (UB) for the case without an additional exclusion zone. Here, we can see that with an aperture of a limited size on Eve's side, the achievable secure key rate outperformed that of the unrestricted case. The lower bound and upper bound were quite close, which gave the range for the capacity. We can also see that an exclusion zone helped increase the key rate when the transmission distance was not too large. However, when the transmission distance was sufficiently large, the lower and upper bounds became constant, as proved in [30], when the collecting ability of Bob and Eve became proportional to their aperture sizes:

$$\lim_{L\to\infty} \frac{P_{Eve}}{P_{Bob}} = \frac{A_e}{A_b}, \tag{8}$$

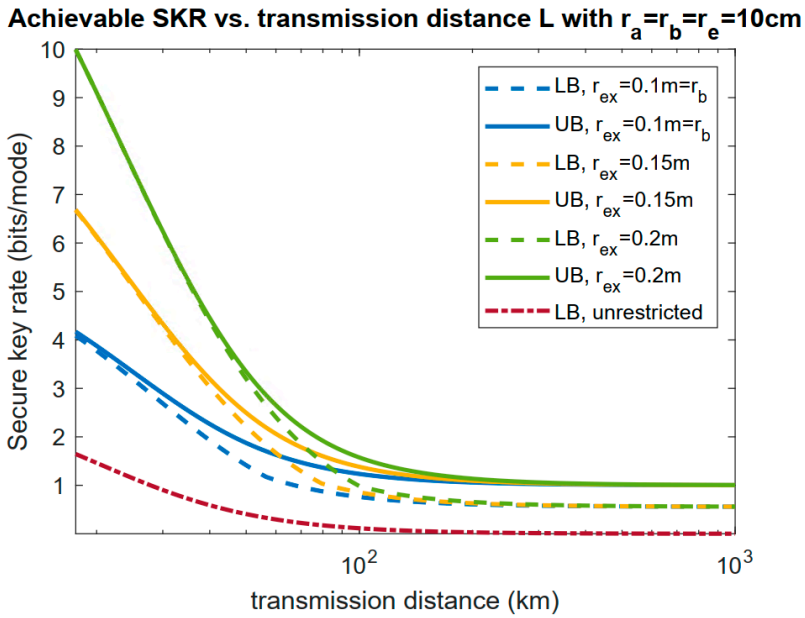

Figure 4. Achievable secure key rate lower and upper bounds as functions of the transmission distance. The unrestricted case (infinite size aperture on Eve's side with $r_{ex} = r_b$) is also included. Here, $W_0 = r_a = r_b = r_e = 10$ cm.

Here, we can see that an exclusion zone would not affect this saturation very much, as at a large transmission distance, the collecting ability of Bob and Eve became proportional to their aperture sizes as in Equation (8) when the area of an exclusion zone was not significantly larger than the receiver aperture sizes of Bob and Eve.

3.2. Eavesdropper's Strategy: A Dynamically Positioned Aperture

In this subsection, we introduce and analyze one of the eavesdropper's possible strategies with a dynamically positioned aperture, which would apply to the geometrical optics restricted model, where Eve could dynamically position her aperture behind Bob's. As is illustrated in Figure 5, $A_{Alice}(A_a)$, $A_{Bob}(A_b)$, and $A_{Eve}(A_e)$ are the area of Alice's aperture (radius r_a), Bob's aperture (radius r_b), and Eve's aperture (radius r_e), respectively. L_{AB} is the distance between Alice's and Bob's aperture planes, while L_{BE} is the distance between Bob's and Eve's aperture planes. D is the distance between Eve's aperture center and the beam propagation line-of-sight path.

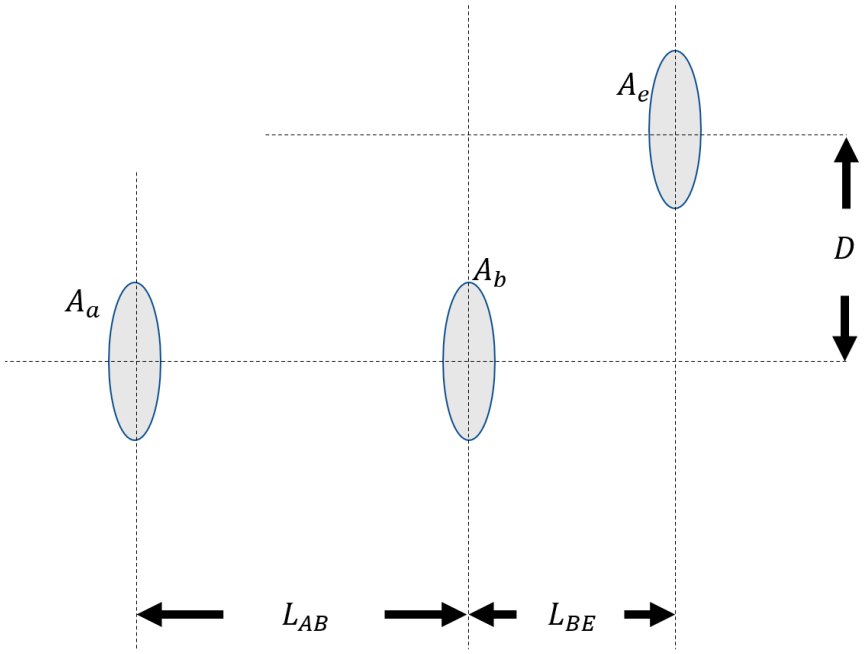

Figure 5. Eavesdropper dynamic positioning set-up.

As was proven in Equation (44) of [33], when L_{AB} was sufficiently large, the optimal strategy for Eve was to set $L_{BE} = L_{AB}$ and $D = 0$. Thus, we set $L_{BE} = L_{AB}$, $D = 0$ and obtained the lower and upper bounds on the achievable secure key rate as in Figure 6. It is shown that in this case, the rate increased with the increase in W_0 as this decreased the divergence angle, making the beam more focused on Bob's aperture plane. We can also see that Eve suppressed Alice and Bob's achievable key rate compared with the similar distance range in Figure 4 by applying this strategy.

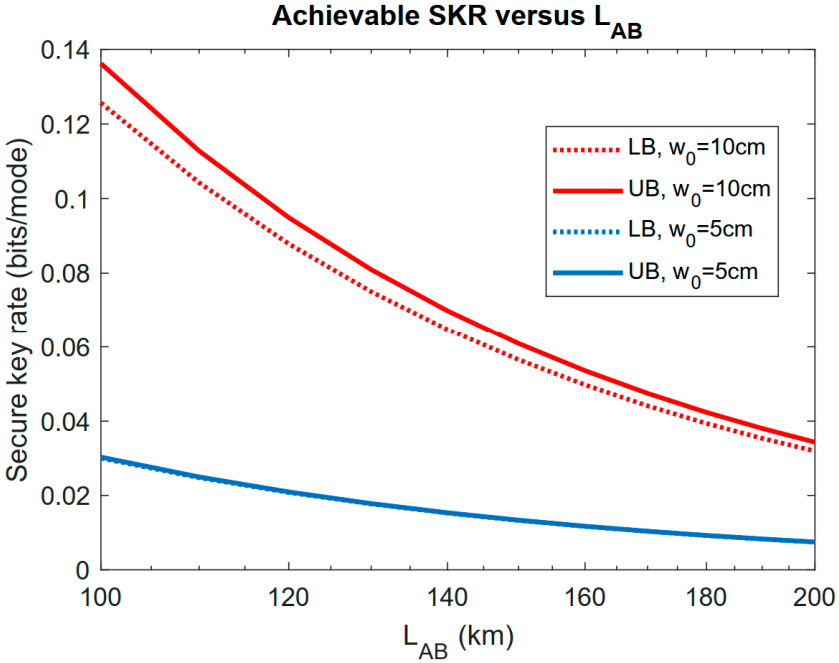

Figure 6. Lower and upper bounds of the achievable secure key rate versus L_{AB} with $L_{BE} = L_{AB}$ and $D = 0$. Bob's and Eve's aperture radii are $r_b = r_e = 10$ cm.

4. Discussion

In this invited paper, we briefly introduced the geometrical optics restricted model and presented a few cases applying this model to some common cases in free-space optical links such as the satellite-to-satellite channel. We showcased the achievable secure key rate lower and upper bounds and compared them to the unrestricted case. Furthermore, we investigated the strategy from both the communication parties' side and Eve's side within this model.

Funding: National Science Foundation (1828132, 1907918).

Acknowledgments: The authors thankfully acknowledge helpful discussions with Saikat Guha, Kaushik P. Seshadreesan and John Gariano from the University of Arizona, Jeffrey H. Shapiro from the Massachusetts Institute of Technology and William Clark and Mark R. Adcock from General Dynamics.

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

References

1. Charles, H.B.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *arXiv* **2020**, arXiv:2003.06557.
2. Dominic, M.; Andrew, C.-C.Y. Quantum Cryptography with Imperfect Apparatus. In Proceedings of the IEEE Symposium on Foundations of Computer Science (FOCS), Palo Alto, CA, USA, 8–11 November 1998.
3. Jonathan, B.; Hardy, L.; Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **2005**, *95*, 010503.
4. Pironio, S.; Acín, A.; Brunner, N.; Gisin, N.; Massar, S.; Scarani, V. Device-independent quantum key distribution secure against collective attacks. *New J. Phys.* **2009**, *11*, 045021. [CrossRef]
5. McKague, M. Device independent quantum key distribution secure against coherent attacks with memoryless measurement devices. *New J. Phys.* **2009**, *11*, 103037. [CrossRef]
6. Mafu, M.; Dudley, A.; Goyal, S.; Giovannini, D.; McLaren, M.; Padgett, M.J.; Konrad, T.; Petruccione, F.; Lütkenhaus, N.; Forbes, A. Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Phys. Rev. A* **2013**, *88*, 032305. [CrossRef]
7. Ziwen, P.; Cai, J.; Wang, C. Quantum key distribution with high order fibonacci-like orbital angular momentum states. *Int. J. Theor. Phys.* **2017**, *56*, 2622–2634.
8. Ivan, B.D. Deep-space and near-Earth optical communications by coded orbital angular momentum (OAM) modulation. *Opt. Express* **2011**, *19*, 14277–14289.
9. Tittel, W.; Brendel, J.; Zbinden, H.; Gisin, N. Quantum cryptography using entangled photons in energy-time Bell states. *Phys. Rev. Lett.* **2000**, *84*, 4737. [CrossRef]
10. Bing, Q. Single-photon continuous-variable quantum key distribution based on the energy-time uncertainty relation. *Opt. Lett.* **2006**, *31*, 2795–2797.
11. Wang, X.-B. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. *Phys. Rev. A* **2005**, *72*, 012322. [CrossRef]
12. Lo, H.-K.; Ma, X.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef] [PubMed]
13. Ma, X.; Qi, B.; Zhao, Y.; Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **2005**, *72*, 012326. [CrossRef]
14. Lutkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **2000**, *61*, 052304. [CrossRef]
15. Cerf, N.J.; Lévy, M.; Van Assche, G. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* **2001**, *63*, 052311. [CrossRef]
16. Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef] [PubMed]
17. Braunstein, S.L.; Van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **2005**, *77*, 513–577. [CrossRef]
18. Maurer, U.M. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory* **1993**, *39*, 733–742. [CrossRef]
19. Michał, H.; Horodecki, P.; Horodecki, R. Unified approach to quantum capacities: Towards quantum noisy coding theorem. *Phys. Rev. Lett.* **2000**, *85*, 433.
20. Devetak, I.; Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A Math. Phys. Eng. Sci.* **2005**, *461*, 207–235. [CrossRef]
21. Renato, R.; Cirac, J.I. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.* **2009**, *102*, 110504.
22. García-Patrón, R.; Pirandola, S.; Lloyd, S.; Shapiro, J.H. Reverse Coherent Information. *Phys. Rev. Lett.* **2009**, *102*, 210501. [CrossRef]
23. Pirandola, S.; García-Patrón, R.; Braunstein, S.L.; Lloyd, S. Direct and Reverse Secret-Key Capacities of a Quantum Channel. *Phys. Rev. Lett.* **2009**, *102*, 050503. [CrossRef]

24. Masahiro, T.; Guha, S.; Wilde, M.M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **2014**, *5*, 1–7.
25. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 15043. [CrossRef] [PubMed]
26. Pan, Z.; Seshadreesan, K.P.; Clark, W.; Adcock, M.R.; Djordjevic, I.B.; Shapiro, J.H.; Guha, S. Secret-Key Distillation across a Quantum Wiretap Channel under Restricted Eavesdropping. *Phys. Rev. Appl.* **2020**, *14*, 024044. [CrossRef]
27. Pan, Z.; Seshadreesan, K.P.; Clark, W.; Adcock, M.R.; Djordjevic, I.B.; Shapiro, J.H.; Guha, S. Secret key distillation over a pure loss quantum wiretap channel under restricted eavesdropping. In Proceedings of the 2019 IEEE International Symposium on Information Theory (ISIT), Paris, France, 7–12 July 2019.
28. Pan, Z.; Djordjevic, I.B. Security of satellite-based cv-qkd under realistic assumptions. In Proceedings of the 2020 22nd International Conference on Transparent Optical Networks (ICTON), Bari, Italy, 19–23 July 2020; pp. 1–4.
29. Pan, Z.; Gariano, J.; Djordjevic, I.B. Secret key distillation over satellite-to-satellite free-space channel with eavesdropper dynamic positioning. In *Signal Processing in Photonic Communications*; Optical Society of America: Washington, DC, USA, 2020; p. SpTu3I-4.
30. Pan, Z.; Djordjevic, I.B. Secret key distillation over satellite-to-satellite free-space optics channel with a limited-sized aperture eavesdropper in the same plane of the legitimate receiver. *Opt. Express* **2020**, *28*, 37129–37148. [CrossRef] [PubMed]
31. Pan, Z.; Gariano, J.; Clark, W.; Djordjevic, I.B. Secret key distillation over realistic satellite-to-satellite free-space channel. In *Quantum 2.0*; Optical Society of America: Washington, DC, USA, 2020; p. QTh7B-15.
32. Pan, Z.; Djordjevic, I.B. Secret key distillation over realistic satellite-to-satellite free-space channel: Exclusion zone analysis. *arXiv* **2020**, arXiv:2009.05929.
33. Pan, Z.; Djordjevic, I.B. Secret Key Distillation over Satellite-to-satellite Free-space Optics Channel with Eavesdropper Dynamic Positioning. *arXiv* **2020**, arXiv:2012.13865.
34. Johns, M.; McCarthy, P.; Raybould, K.; Bouchez, A.; Farahani, A.; Filgueira, J.; Jacoby, G.; Shectman, S.; Sheehan, M. Giant magellan telescope: Overview. In *Ground-Based and Airborne Telescopes IV, Volume 8444*; International Society for Optics and Photonics: Amsterdam, The Netherlands, 2012; p. 84441H.
35. Montagnino, L.A. Test and evaluation of the hubble space telescope 2.4-meter primary mirror. In *Large Optics Technology, Volume 571*; International Society for Optics and Photonics: San Diego, CA, USA, 1985; pp. 182–190.
36. Wright, E.L.; Eisenhardt, P.R.M.; Mainzer, A.K.; Ressler, M.E.; Cutri, R.; Jarrett, T.; Kirkpatrick, D.; Padgett, D.; McMillan, R.S.; Skrutskie, M.; et al. The wide-field infrared survey explorer (wise): Mission description and initial on-orbit performance. *Astron. J.* **2010**, *140*, 1868–1881. [CrossRef]