entropy

MDPI

Review

An Overview of Geometrical Optics Restricted Quantum Key Distribution

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@email.arizona.edu
* Correspondence: ziwenpan@email.arizona.edu

Abstract: Quantum key distribution (QKD) assures the theoretical information security from the physical layer by safely distributing true random numbers to the communication parties as secret keys while assuming an omnipotent eavesdropper (Eve). In recent years, with the growing applications of QKD in realistic channels such as satellite-based free-space communications, certain conditions such as the unlimited power collection ability of Eve become too strict for security analysis. Thus, in this invited paper, we give a brief overview of the quantum key distribution with a geometrical optics restricted power collection ability of Eve with its potential applications.

Keywords: quantum key distribution; satellite; free-space channel

Citation: Pan, Z.; Djordjevic, I.B. An Overview of Geometrical Optics Restricted Quantum Key Distribution. *Entropy* **2021**, *23*, 1003. https://doi.org/10.3390/e23081003

Academic Editor: Steeve Zozor

Received: 29 June 2021
Accepted: 27 July 2021
Published: 31 July 2021

1. Introduction

There has been a long history of cryptography [1–6]. Before the 20th century, cryptography was considered as an art that mainly relies on personal skills to construct or break codes, without proper theoretical study [7]. Focused on message confidentiality, classical cryptography was known to ensure secrecy in communications under different situations such as military or diplomat use or between spies. An important representative of classic cryptography is transposition ciphers, which rearrange the message to hide the original meanings. After the early 20th century, following the establishment of the information theory by Harry Nyquist, Ralph Hartley, and Claude Shannon [8–13], the study of cryptography started to exploit the tools of mathematics. Cryptography also became a branch of engineering, especially after the use of computers, which allows binary encryption of data. Two major schemes of modern cryptography include symmetric (private-key) cryptography, e.g., the Data Encryption Standard (DES) [14] and Advanced Encryption Standard (AES) [15], and asymmetric (public-key) cryptography, e.g., RSA algorithm [16]. Symmetric cryptography relies on the shared key between the communication parties (Alice and Bob), whereas in asymmetric cryptography, the encryption keys are different from decryption keys. In general, symmetric cryptography is more efficient than asymmetric cryptography with more concise designs, but it has difficulties when it comes to the safe distribution of the shared keys. On the other hand, asymmetric cryptography using a public key and a private key for encryption and decryption, respectively, relies upon mathematical problems termed one-way functions that are computationally infeasible from one direction (public key) [17], and are more widely used today for avoiding the risky stage of safe distribution of keys in symmetric cryptography.

However, with the fast development of quantum computing [18] and its potential in solving conventional one-way functions, it is possible to break the current encryption systems [19] with algorithms such as Shor's algorithm [20] and Grover's algorithm [21]; thus, the QKD is now becoming more and more important in the new era of information security. Different from the asymmetric cryptography used today, QKD is based on symmetric cryptography, guaranteeing the secure distribution of the secret keys with the laws of quantum mechanics that the measurement process generally disturbs the

measured system. This can be used to detect eavesdropping actions as any adversaries would have to perform measurement to eavesdrop. Since the study of the first QKD protocol BB84 [2], the theory of QKD has vastly developed, with numerous protocols proposed [3–5,22–32] to improve security and increase secure-key rate (SKR). Combined with the one-time pad proved to be asymptotically safe in 1949 by Claude Shannon [1], QKD promises completely secure communication. On the other hand, QKD conventionally assumes that Eve is only limited by the laws of physics even though some assumptions might be unrealistic. For example, Eve is always assumed to have the ability to collect all photons that do not arrive at Bob's receiver, which would make sense in cases such as fiber communication but would be too strict for wireless communication cases. Thus, interest has been rising surrounding the study of QKD with more realistic power collection assumptions and its potential applications [33–40].

In this invited paper, we present an overview of the geometrical optics restricted quantum key distribution with certain power collection restrictions applied on Eve. We start by reviewing the conventional QKD studies in Section 2 with different protocols and compare the achievable secure-key rate between the famous discrete variable protocol BB84 with decoy states added and the continuous variable Gaussian modulated QKD scheme. Then, in Section 3, we introduce the geometrical optics restricted model by limiting Eve's collectable power with a beam splitter and showcase the lower bound results in this model. After that, we present some possible applications of this model by studying some representative scenarios with it.

2. Quantum Key Distribution (QKD)

With the fast development of potential applications of QKD such as quantum networks [41,42] and satellite-based quantum secure communication [43–47], various protocols have been proposed aimed at improved security while assuming an all-powerful eavesdropper. For example, the first QKD protocol BB84 was studied in 1984 by Charles H. Bennett et al. to use polarization states to securely distribute secret keys [2]. It was also known as the first prepare-and-measure (PM) model as it exploits the result of quantum indeterminacy that measuring an unknown quantum state in general changes the state. It was then simplified to the B92 protocol by using two non-orthogonal states [3] before extending to its entanglement-based (EB) version BBM92 [4] in 1992.

Different from the PM models, the EB models use entangled pairs in the transmission stage to distribute secret keys to the two communication parties. BBM92 was also considered as an improvement to the first EB model E91 [5], which uses three mutually unbiased bases instead of two in BBM92. There was also an important equivalence established between PM and EB models in [4] that the security proof of one implies the same for the other.

However, when it comes to device-independent (DI) studies, EB models have advantages over PM models [23] since the security proofs of DI-QKD are mainly based on the violation of Bell inequalities [48–51]. Some PM models are proven to be partially DI [52] The device independence study was first proposed in [6] using internal operations to "self-test" quantum apparatus. Different protocols have since been studied [22–24].

Another important category of quantum key distribution protocols is the continuous-variable (CV-) QKD. Different from most protocols described above, which are called discrete-variable (DV) protocols that rely on single photon sources and single photon detectors, CV protocols encode keys into CV observables of light fields [53]. This enabled CV protocols to be more easily implementable as it is compatible with most current communication devices. The first protocol using squeezed states [25] was proposed in 2000, which generalizes the BB84 protocol using squeezed states. In 2002, another important CV protocol GG02 using Gaussian modulated coherent states [26] was proposed as coherent states are much easier to generate experimentally.

Other interesting directions in QKD research include using decoy states [27–29,54] against photon number splitting (PNS) attack [55] where the eavesdropper exploits the

loophole of a non-ideal single photon transmission; finite-size analysis [56] where the transmitted sequence is not large enough for asymptotic security analysis; measurement-device-independent (MDI-) QKD [57] that comes from DI-QKD but assumes perfect preparation of the states; and high-dimensional QKD that exploits high dimensional degrees of freedom such as the orbital angular momentum (OAM) [30–32] and the temporal-spectral [58,59] aimed at increasing key rates, etc. Here we present introductions to two representatives in DV and CV protocols:

2.1. BB84

BB84 protocol uses single photons to distribute secret keys. First, Alice randomly prepares a sequence chosen from two sets of orthogonal bases as in Figure 1 and sends them to Bob.

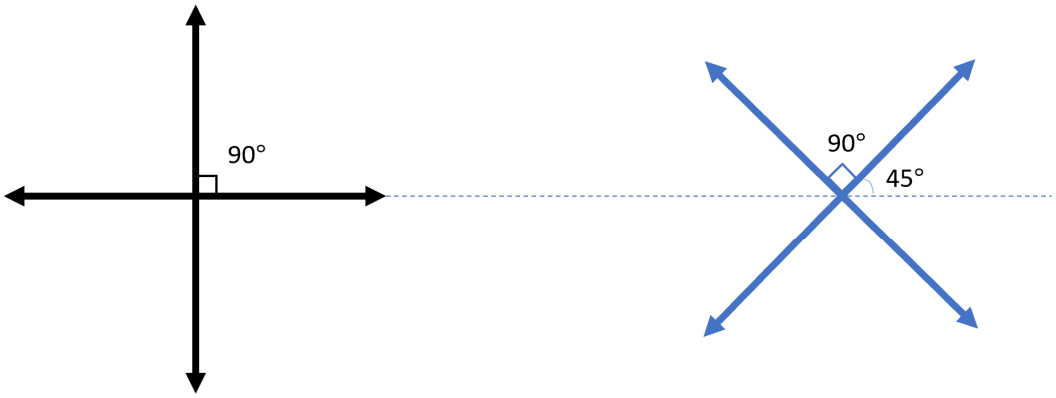


Figure 1. BB84 polarization bases.

Next, Bob would also randomly choose from these two sets of orthogonal bases to measure the received photons. After completing the measurements, Bob would report his basis of measurement. If Alice's preparing basis is the same as Bob's measurement basis, then the result should be the same, which would be the sifted keys.

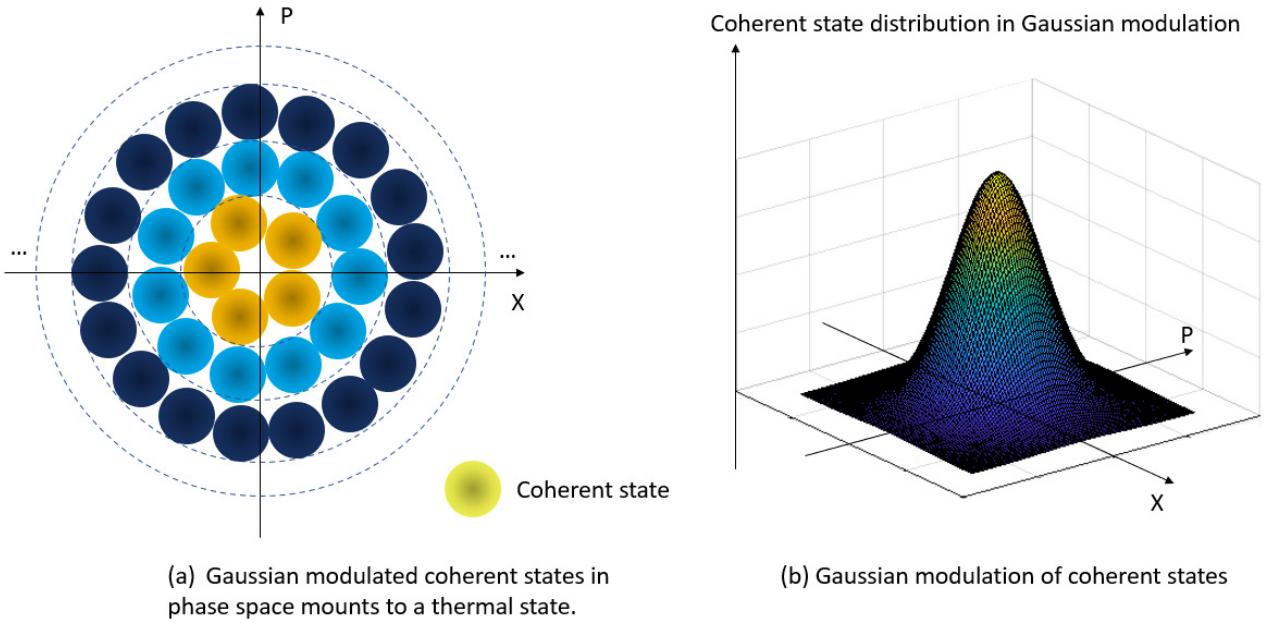
If Eve intercepts the photons transmitted, performs a measurement of her own, and resends the photons to Bob, then when Eve's measurement basis is not the same as Alice's and Bob's, the polarization state would be changed so that the sifted keys would be different on Alice's and Bob's side. Thus, either Alice or Bob can reveal some of the sifted keys publicly for the other party to compare and detect possible eavesdropping. An illustrative example of this process is shown in Table 1.

Table 1. BB84 protocol process illustration.

Random Bits	**0**	**1**	**0**	**0**	**1**	**1**	**1**	**0**	**1**
Alice basis	a	a	b	a	b	a	b	b	a
Polarization state sent	↔	↕	⤡	↔	⤢	↕	⤢	⤡	↕
Bob basis	b	a	a	b	b	a	b	a	b
Bob measurement results	random	↕	random	random	⤢	↕	⤢	random	random
Sifted keys		1			1	1	1		

2.2. GG02

GG02 protocol uses Gaussian modulated coherent states, as in Figure 2, to distribute secret keys. First, Alice generates random real number pairs (a_x, a_p) from two independent Gaussian distributions with given modulation variances and sends them to Bob. Next, Bob randomly chooses to measure either x or p quadrature components.



(a) Gaussian modulated coherent states in phase space mounts to a thermal state.

(b) Gaussian modulation of coherent states

Figure 2. Gaussian modulated coherent states distributed on phase space.

After all the transmission and measurements are done, Bob discloses for each measurement whether he measured x or p components. Then, Alice retains the corresponding a_x and a_p values. Secret keys can then be extracted with certain reconciliation and privacy amplification.

For these protocols, if Bob is the one performing the measurement and Alice is post-processing its outcomes to infer Bob's encodings, assisted by classical communications from Bob to Alice, this is the reverse reconciliation scheme. Otherwise, it is the direct reconciliation scheme. Here we present a secure key rate lower bound (achievable rate) comparison between CV Gaussian modulation protocol with coherent states, heterodyne detection, reverse reconciliation, and DV protocol Decoy-State (DS-) BB84, of which detailed calculations can be found in [33,60]. We assume that a weak coherent-state source with signal-state pulses is used which transmits μ photons per pulse on average at a rate R states per second over an Alice-to-Bob channel with overall transmissivity η. Thermal noise is denoted as ne per mode.

In Figure 3a,b, the reconciliation efficiency β for CV protocol and f_L for DV protocol are both set to one. By comparing Figure 3a,c, we can see that in a pure loss channel ($ne = 0$), the CV protocol always outperforms its DV counterpart. However, when thermal noise is non-zero, DV can outperform CV, especially when reconciliation is not perfect. We can also compare DV and CV results with input power optimized, as in Figure 4, where the input power is optimized correspondingly with perfect reconciliation. We can see that although Gaussian-modulated CV protocol has advantages over DS-BB84 on the secure key rate, it does not outperform DS-BB84 when it comes to the transmission distance as channel loss increases with increasing transmission distance.

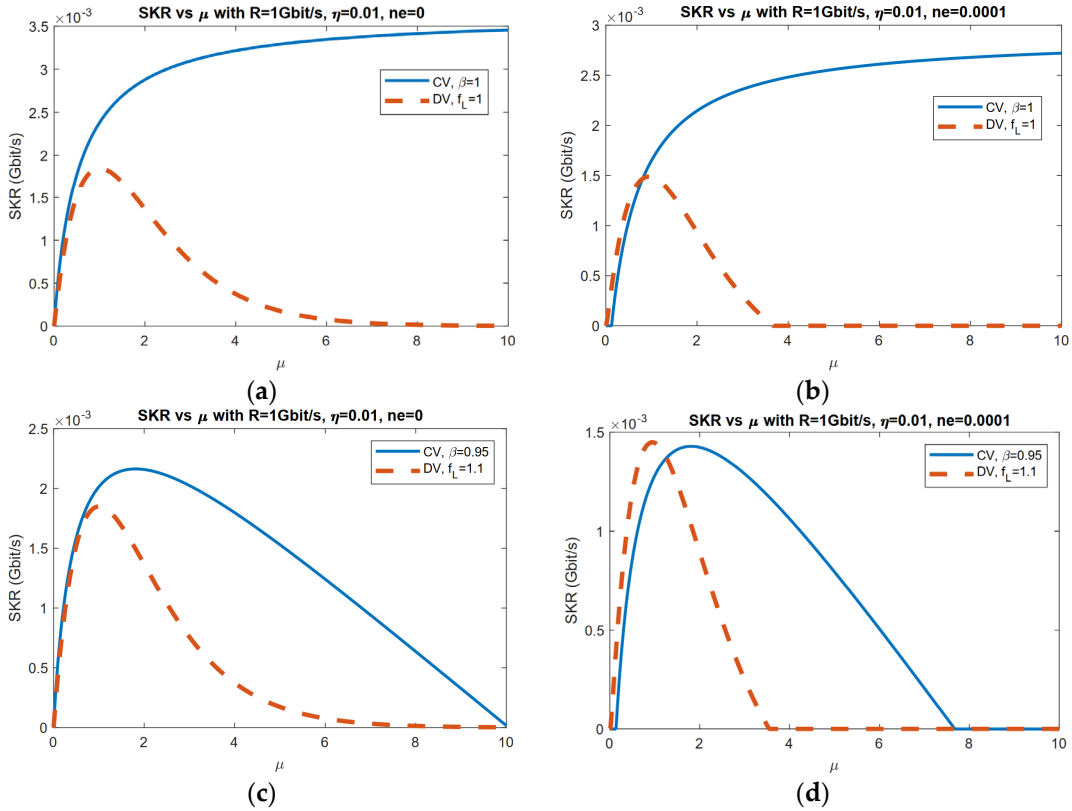


Figure 3. Comparison of CV Gaussian modulation protocol with coherent states, heterodyne detection, reverse reconciliation, and DV protocol DS-BB84 with mean photon number per input mode. (**a**) Perfect reconciliation in pure loss channel. (**b**) Perfect reconciliation with $ne = 0.0001$. (**c**) Imperfect reconciliation in pure loss channel. (**d**) Imperfect reconciliation with $ne = 0.0001$.

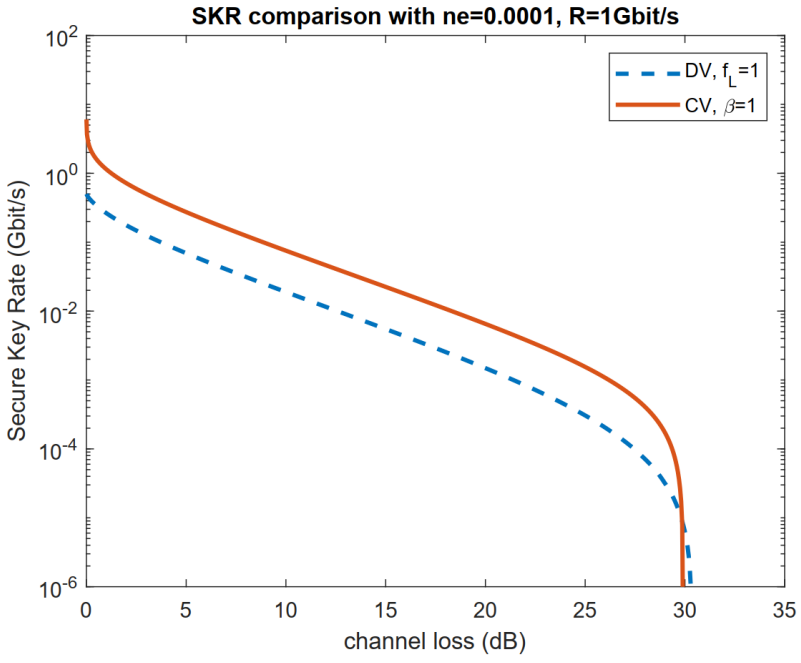


Figure 4. Comparison of CV Gaussian modulation protocol with coherent states, heterodyne detection, reverse reconciliation, and DV protocol DS-BB84 with channel loss. Here the input power is optimized correspondingly. Reconciliation is perfect for both CV and DV protocols.

3. Geometrical Optics Restricted Model

In this section, we introduce the geometrical optics restricted model with realistic power collection restriction on the eavesdropper. In [33], a wiretap channel is used to denote the power collection restriction on Eve as in Figure 5. Here the beam splitter with transmissivity κ denotes that Eve can only collect κ fraction of the photons that do not arrive at Bob's receiver. The Alice-to-Bob channel is with transmissivity η.

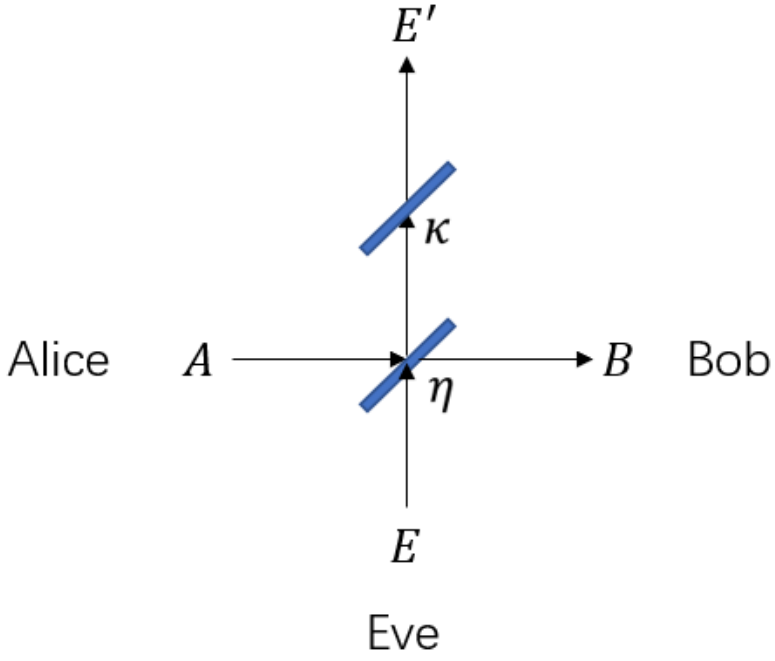


Figure 5. The wiretap channel notation of the geometrical optics restricted model.

Similar notations have been seen in broadcast channel studies [61,62]. Starting from the Hashing inequality [63] the lower bound on the secure key rate for both direct and reverse reconciliation were derived without a specified detection scheme on one of the communication parties:

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

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

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

where detailed expressions of $\nu_{y_i}^{ER}$ can be found in [33].

Here we reproduce the comparison in Figure 4 between DV protocol DS-BB84 and CV Gaussian modulation protocol with coherent states, heterodyne detection, and reverse reconciliation as in Figure 6. We retain the results from Figure 4, as $\kappa = 1$ case and plotted the DV and CV rate with $\kappa = 0.5$. We can see an increase in the achievable rate in both CV and DV protocols and that the CV protocol only holds advantages over the DV protocols when channel loss is small. We can also see that when $\kappa = 0.5$, the rate goes to zero at a larger channel loss, suggesting larger transmission distance in this case.

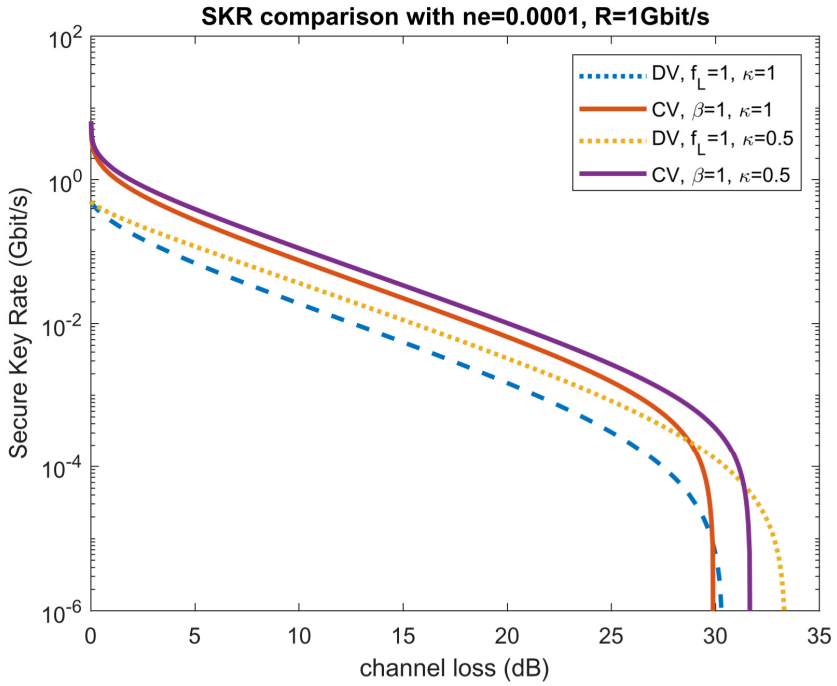


Figure 6. DV protocol DS-BB84 and CV Gaussian modulation protocol with coherent states, heterodyne detection, and reverse reconciliation SKR comparison with input power optimized.

The geometrical optics restricted model has multiple potential applications in different scenarios of practical importance. Here we present some possible directions.

3.1. Application of Geometrical Optics Restricted Model: Limited Aperture Size Analysis

Different from the assumptions in conventional QKD study that Eve is unlimited in her ability of power collection, in most realistic application scenarios, especially in wireless communication, Eve is limited by her receiver aperture size. Taking free-space optical communication link as an example, the receiver aperture size usually ranges from a few centimeters to a few decimeters. If we only restrict Eve's aperture size but grant her mobility of her aperture, which could be accomplished through unmanned aerial vehicle (UAV) or usage of a spy satellite during satellite communications, we can study the security of specific application occasions.

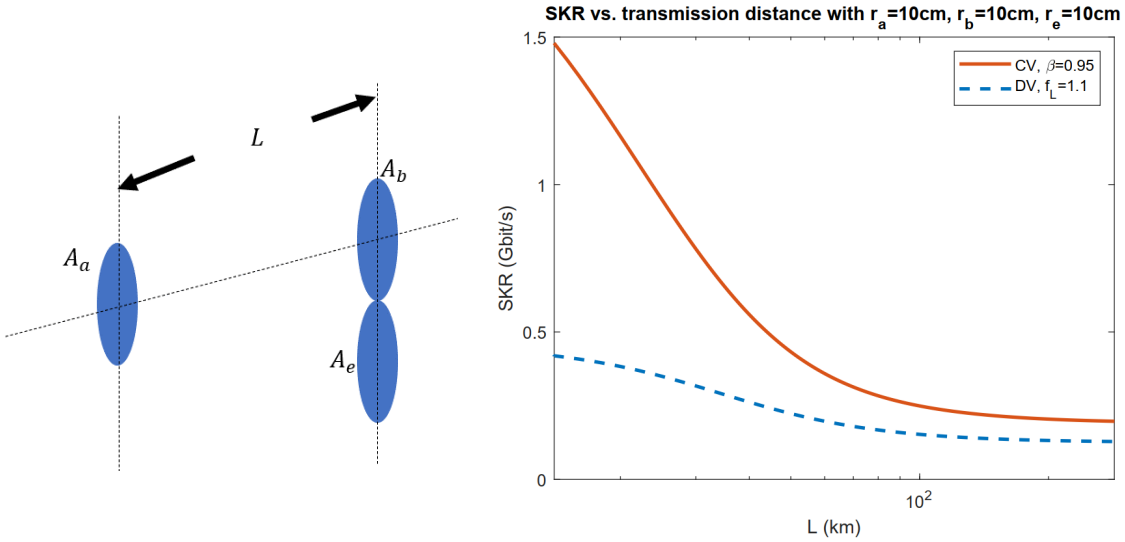
In [35,37,38], the straightforward case scenario of a limited-sized aperture of Eve is considered where Eve places her aperture beside Bob's receiver in a satellite-to-satellite communication scheme as in Figure 7a. It is shown in Figure 7b that the rate tends to be a constant when the transmission distance is sufficiently large.

This was also derived in detail as in Equations (4) and (5), where m is the ratio of Eve's aperture size versus Bob's aperture size.

$$\lim_{\mu\to\infty, L\to\infty} K_{\rightarrow} \geq -\log_2 m \tag{4}$$

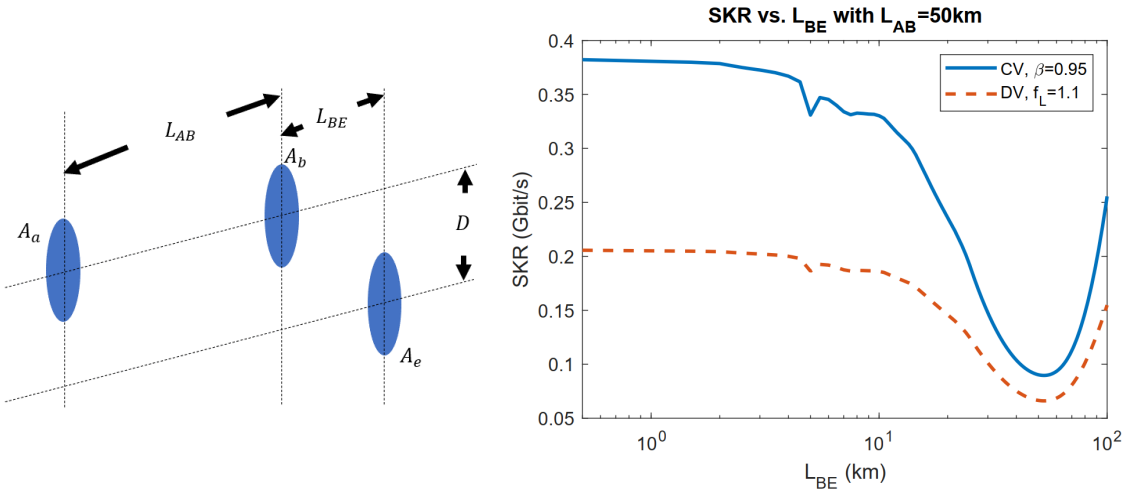
$$\lim_{\mu\to\infty, L\to\infty} K_{\leftarrow} \geq -\log_2 \frac{m}{m+1}^{1+m} e \tag{5}$$

In [36,40], the case with dynamically positioned eavesdropper aperture is considered with Eve's position being optimized, as in Figure 8a. In Figure 8b, both CV and DV lower bounds are presented with optimized Eve's position. Assuming the Gaussian beam is transmitted, because of the cylindrical symmetry of a Gaussian beam, the distance D between Eve's aperture to the beam transmission axis can be used to denote Eve's position combined with Bob-to-Eve distance L_{BE}. It is clear that by optimizing Eve's position, advantages over Alice and Bob can be further obtained by Eve compared with Figure 7b.



(**a**) (**b**)

Figure 7. (**a**) Setup of the limited aperture scenario. A_a, A_b, A_e respectively refer to the aperture area of Alice (radius r_a), Bob (radius r_b), and Eve (radius r_e). L is the distance between Alice's aperture and Bob's. (**b**) CV and DV SKR lower bounds versus transmission distance with optimized input power. Gaussian beam with beam waist $W_0 = r_a$ and wavelength $\lambda = 1550$ nm is transmitted. The space temperature is set to $T = 3$ K.



(**a**) (**b**)

Figure 8. (**a**) Setup of the dynamic positioning of Eve. A_a, A_b, A_{Eve} respectively refer to the aperture area of Alice (radius r_a), Bob (radius r_b), and Eve (radius r_e). L_{AB} is the distance between Alice's aperture and Bob's. L_{BE} is the distance between Bob's aperture and Eve's. (**b**) CV and DV lower bound secret keys versus Bob-to-Eve distance L_{BE} with Alice-to-Bob distance $L_{AB} = 50$ km. Gaussian beam with beam waist $W_0 = r_a = r_b = r_e = 10$ cm and wavelength $\lambda = 1550$ nm is transmitted. The space temperature is set to $T = 3$ K.

3.2. Application of Geometrical Optics Restricted Model: Exclusion Zone Analysis

From the defense point of view, one of the most effective ways to suppress Eve's power collection ability is to set an exclusion zone around the legitimate receiver. In [39] an exclusion zone is assumed to be set surrounding the legitimate receiver, excluding the eavesdropper Eve from collecting photons in this region, as in Figure 9a. In Figure 9b, an exclusion zone is shown to increase the secure key rate for both CV and DV protocols, but this is more effective when the transmission distance is not too large.

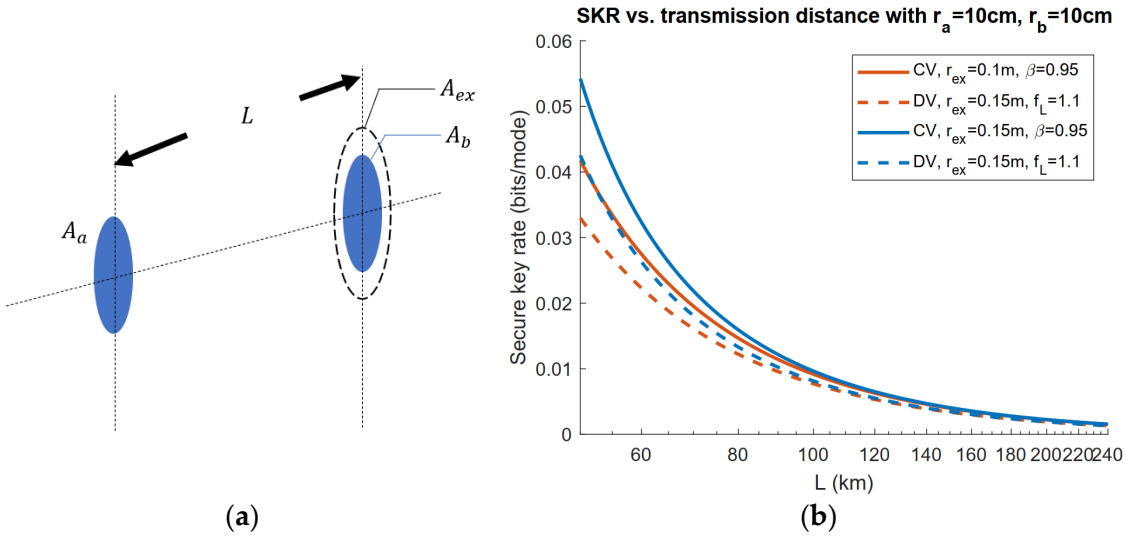


Figure 9. (**a**) Setup of exclusion zone scenario. A_a, A_b, A_{ex} respectively refer to the area of Alice's aperture (radius r_a), Bob's aperture (radius r_b), and the exclusion zone (radius r_{ex}). L is the distance between Alice's aperture and Bob's. (**b**) CV and DV lower bound of secret keys versus transmission distance L with or without an exclusion zone. Gaussian beam with beam waist $W_0 = r_a$ and wavelength $\lambda = 1550$ nm is transmitted. The space temperature is set to $T = 3$ K.

4. Discussion

In this paper, we provided a brief overview of the geometrical optics restricted QKD and discussed its potential applications. We started by reviewing some of the existing QKD schemes before going into the geometrical optics restricted model notation in a wiretap channel that can better characterize the power collection state of some realistic scenarios instead of attributing too much power to Eve. After we introduced the lower bound results in this model, we then presented some of the application directions of this model, mostly in free-space channels such as satellite communication. We showcased selected results from both Eve's side with her optimized position strategy and the communication parties' side with an exclusion zone as a defense strategy.

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 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. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
2. Bennett, C.H.; Gilles, B. Quantum cryptography: Public key distribution and coin tossing. *Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
3. Bennett, C.H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **1992**, *21*, 3121. [CrossRef] [PubMed]
4. Bennett, C.H.; Gilles, B.; Mermin, N.D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **1992**, *68*, 557. [CrossRef] [PubMed]
5. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661. [CrossRef] [PubMed]
6. Mayers, D.; Yao, A. Quantum Cryptography with Imperfect Apparatus. In Proceedings of the 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280), Palo Alto, CA, USA, 8–11 November 1998.
7. Katz, J.; Yehuda, L. *Introduction to Modern Cryptography*; CRC Press: Boca Raton, FL, USA, 2020.
8. Nyquist, H. Regeneration theory. *Bell Syst. Tech. J.* **1932**, *11*, 126–147. [CrossRef]
9. Nyquist, H. Certain factors affecting telegraph speed. *Bell Syst. Tech. J.* **1924**, *3*, 324–346. [CrossRef]
10. Nyquist, H. Certain topics in telegraph transmission theory. *Trans. AIEE* **1928**, *47*, 617–644, Reprint as classic paper in *Proc. IEEE* **2002**, *90*, 280–305. [CrossRef]
11. Hartley, R.V.L. Relations of Carrier and Side-Bands in Radio Transmission. *Proc. IRE* **1923**, *11*, 34–56. [CrossRef]
12. Hartley, R.V.L. Transmission of Information. *Bell Syst. Tech. J.* **1928**, *7*, 535–563. [CrossRef]

13. Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423. [CrossRef]
14. Data Encryption Standard. Available online: https://telluur.com/utwente/master/SyS%20-%20System%20Security/2018/Aanvullende%20docs/Data_Encryption_Standard.pdf (accessed on 28 July 2021).
15. Advanced Encryption Standard. Available online: https://telluur.com/utwente/master/SyS%20-%20System%20Security/2018/Aanvullende%20docs/AES.pdf (accessed on 28 July 2021).
16. Rivest, R.L.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM.* **1978**, *21*, 120–126. [CrossRef]
17. Diffie, W.; Hellman, M. New Directions in Cryptography (PDF). *IEEE Trans. Inf. Theory* **1976**, *6*, 644–654. [CrossRef]
18. Preskill, J. Quantum Computing in the NISQ era and beyond. *Quantum* **2018**, *2*, 79. [CrossRef]
19. Mavroeidis, V.; Kamer, V.; Mateusz, D.Z.; Audun, J. The impact of quantum computing on present cryptography. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 405–414. [CrossRef]
20. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Washington, DC, USA, 20–22 November 1994.
21. Grover, L.K. A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; pp. 212–219.
22. Barrett, J.; Hardy, L.L.; Kent, A.A. No Signaling and Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *95*, 010503. [CrossRef]
23. 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]
24. McKague, M. Device independent quantum key distribution secure against coherent attacks with memoryless meas-urement devices. *New J. Phys.* **2009**, *11*, 103037. [CrossRef]
25. Cerf, N.J.; Lévy, M.; Van Assche, G. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* **2001**, *63*, 052311. [CrossRef]
26. Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef]
27. Wang, X.-B. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. *Phys. Rev. A* **2005**, *72*, 012322. [CrossRef]
28. Lo, H.-K.; Ma, X.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef]
29. Ma, X.; Qi, B.; Zhao, Y.; Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **2005**, *72*, 012326. [CrossRef]
30. Mafu, M.; Dudley, A.; Goyal, S.; Giovannini, D.; McLaren, M.; Padgett, M.; Konrad, T.; Petruccione, F.; Lutkenhaus, N.; Forbes, A. Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Phys. Rev. A* **2013**, *88*, 032305. [CrossRef]
31. Pan, Z.; Cai, J.; Wang, C. Quantum Key Distribution with High Order Fibonacci-like Orbital Angular Momentum States. *Int. J. Theor. Phys.* **2017**, *56*, 2622–2634. [CrossRef]
32. Djordjevic, I.B. Deep-space and near-Earth optical communications by coded orbital angular momentum (OAM) modulation. *Opt. Express* **2015**, *19*, 14277–14289. [CrossRef]
33. 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]
34. 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; pp. 3032–3036. [CrossRef]
35. 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.
36. Pan, Z.; Gariano, J.; Djordjevic, I.B. Secret Key Distillation over Satellite-to-satellite Free-space Channel with Eavesdropper Dynamic Positioning. In *OSA Advanced Photonics Congress (AP) 2020 (IPR, NP, NOMA, Networks, PVLED, PSC, SPPCom, SOF)*; The Optical Society: Washington, DC, USA, 2020; p. SpTu3I.4.
37. Pan, Z.; Djordjevic, I.B. Secret key distillation over satellite-to-satellite free-space optics channel with a lim-ited-sized aperture eavesdropper in the same plane of the legitimate receiver. *Opt. Express* **2020**, *28*, 37129–37148. [CrossRef] [PubMed]
38. Pan, Z.; Gariano, J.; Clark, W.; Djordjevic, I.B. Secret key distillation over realistic satellite-to-satellite free-space channel. In Proceedings of the OSA Quantum 2.0 Conference, Washington, DC, USA, 14–17 September 2020; p. QTh7B.15.
39. Pan, Z.; Djordjevic, I.B. Secret key distillation over realistic satellite-to-satellite free-space channel: Exclusion zone analysis. *arXiv* **2020**, arXiv:2009.05929.
40. Pan, Z.; Djordjevic, I.B. Secret Key Distillation over Satellite-to-satellite Free-space Optics Channel with Eaves-dropper Dynamic Positioning. *arXiv* **2020**, arXiv:2012.13865.
41. Fröhlich, B.; Dynes, J.F.; Lucamarini, M.; Sharpe, A.W.; Yuan, Z.; Shields, A.J. A quantum access network. *Nat. Cell Biol.* **2013**, *501*, 69–72. [CrossRef]
42. Kimble, H.J. The quantum internet. *Nat. Cell Biol.* **2008**, *453*, 1023–1030. [CrossRef]
43. Vallone, G.; Bacco, D.; Dequal, D.; Gaiarin, S.; Luceri, V.; Bianco, G.; Villoresi, P. Experimental Satellite Quantum Communications. *Phys. Rev. Lett.* **2015**, *115*, 040502. [CrossRef]

44. Jian-Yu, S.; Yang, B.; Sheng-Kai, L.; Zhang, L.; Shen, Q.; Xiao-Fang, H.; Jin-Cai, W. Direct and full-scale experimental verifications towards ground–satellite quantum key distribution. *Nat. Photonics* **2013**, *7*, 387–393.
45. Liao, S.-K.; Cai, W.-Q.; Liu, W.-Y.; Zhang, L.; Li, Y.; Ren, J.-G.; Yin, J.; Shen, Q.; Cao, Y.; Li, Z.-P.; et al. Satellite-to-ground quantum key distribution. *Nat. Cell Biol.* **2017**, *549*, 43–47. [CrossRef]
46. Bedington, R.; Arrazola, J.M.; Ling, A. Progress in satellite quantum key distribution. *Quantum Inf.* **2017**, *3*, 30. [CrossRef]
47. Ecker, S.; Liu, B.; Handsteiner, J.; Fink, M.; Rauch, D.; Steinlechner, F.; Scheidl, T.; Zeilinger, A.; Ursin, R. Strategies for achieving high key rates in satellite-based QKD. *Npj Quantum Inf.* **2021**, *7*, 1–7. [CrossRef]
48. Pironio, S.; Acín, A.; Massar, S.; Boyer de La Giroday, A.; Matsukevich, N.D.; Maunz, P.; Olmschenk, S. Random numbers certified by Bell's theorem. *Nature* **2010**, *464*, 1021–1024. [CrossRef]
49. Masanes, L.; Pironio, S.; Acín, A. Secure device-independent quantum key distribution with causally in-dependent measurement devices. *Nat. Commun.* **2011**, *2*, 1–7. [CrossRef]
50. Pironio, S.; Masanes, L.; Leverrier, A.; Acín, A. Security of Device-Independent Quantum Key Distribution in the Bounded-Quantum-Storage Model. *Phys. Rev. X* **2013**, *3*, 031007. [CrossRef]
51. Vazirani, U.; Vidick, T. Fully Device Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2014**, *62*, 133. [CrossRef]
52. Pusey, M.F. Verifying the quantumness of a channel with an untrusted device. *J. Opt. Soc. Am. B* **2015**, *32*, A56–A63. [CrossRef]
53. Braunstein, S.L.; Van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **2005**, *77*, 513–577. [CrossRef]
54. Schmitt-Manderbach, T.; Weier, H.; Fürst, M.; Ursin, R.; Tiefenbacher, F.; Scheidl, T.; Perdigues, J. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.* **2007**, *98*, 010504. [CrossRef]
55. Lutkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **2000**, *61*, 052304. [CrossRef]
56. Scarani, V.; Renato, R. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.* **2008**, *100*, 200501. [CrossRef]
57. Lo, H.-K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
58. Tittel, W.; Brendel, J.; Zbinden, H.; Gisin, N. Quantum Cryptography Using Entangled Photons in Energy-Time Bell States. *Phys. Rev. Lett.* **2000**, *84*, 4737–4740. [CrossRef]
59. Qi, B. Single-photon continuous-variable quantum key distribution based on the energy-time uncertainty relation. *Opt. Lett.* **2006**, *31*, 2795–2797. [CrossRef]
60. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 15043. [CrossRef]
61. Takeoka, M.; Seshadreesan, K.P.; Wilde, M.M. Unconstrained distillation capacities of a pure-loss bosonic broadcast channel. In Proceedings of the 2016 IEEE International Symposium on Information Theory (ISIT), Barcelona, Spain, 10–15 July 2016; pp. 2484–2488. [CrossRef]
62. Takeoka, M.; Seshadreesan, K.P.; Wilde, M.M. Unconstrained Capacities of Quantum Key Distribution and Entanglement Distillation for Pure-Loss Bosonic Broadcast Channels. *Phys. Rev. Lett.* **2017**, *119*, 150501. [CrossRef] [PubMed]
63. 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]