Satellite-Based Continuous-Variable Quantum Communications: State-of-the-Art and a Predictive Outlook

Nedasadat Hosseinidehaj, Zunaira Babar, Robert Malaney, Soon Xin Ng, *Senior Member, IEEE,* and Lajos Hanzo, *Fellow, IEEE*

***Abstract*—The recent launch of the Micius quantum-enabled satellite heralds a major step forward for long-range quantum communication. Using single-photon discrete-variable quantum states, this exciting new development proves beyond any doubt that all of the quantum protocols previously deployed over limited ranges in terrestrial experiments can in fact be translated to global distances via the use of low-orbit satellites. In this paper we survey the imminent extension of space-based quantum communication to the continuous-variable regime—the quantum regime perhaps most closely related to classical wireless communications. The continuous variable regime offers the potential for increased communication performance, and represents the next major step forward for quantum communications and the development of the global quantum Internet.**

***Index Terms*—Quantum key distribution, free space optical, satellite communication, continuous variable quantum.**

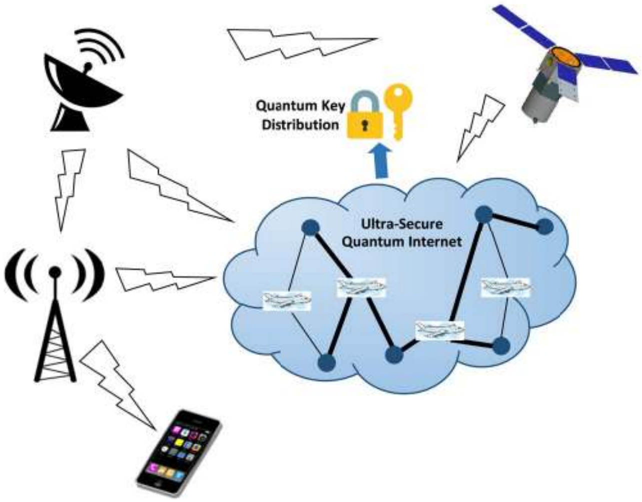


Fig. 1. Stylized vision of future global quantum communications unifying the separate classical and quantum systems into a joint secure universe for anyone, anywhere, anytime.

I. Motivation and Introduction

MOORE'S Law has remained valid for half-a-century! As a result, contemporary semi-conductor technology is approaching nano-scale integration. Hence nano-technology is about to enter the realms of quantum physics, where many of the physical phenomena are rather different from those of classical physics. Hence this treatise contributes towards completing the 'quantum jig-saw puzzle' by paving the way from classical wireless systems to their perfectly secure quantum-communications counterparts, as heralded in [1] and [2].

- *The Inspiration:* In order to circumvent the specific limitations of the classical wireless systems detailed in [1], we set out to bridge the separate classical and quantum worlds into a joint universe, with the objective of contributing to perfectly secure quantum-aided communications for anyone, anywhere, anytime across the globe, as indicated by the stylized vision of the near-future quantum communications scenario seen in Fig. 1.
- *The Reality:* However, quantum processing is far from being flawless - it has substantial challenges, as detailed in this contribution. Nonetheless, at the time of writing long-range quantum communications via satellites has become a reality.

Amongst its numerous intriguing attributes, quantum communication has the potential to achieve secure communications at confidence levels simply unattainable in classical communications settings. This is due to the fact that quantum physics introduces a range of phenomena which have no counterpart in the classical domain, such as quantum entanglement and the superposition of quantum states.[1] The exploitation of such effects, both before and after the transmission of information in the quantum domain, can in effect lead to communications possessing 'unconditional' security.

Manuscript received December 27, 2017; revised June 22, 2018; accepted August 4, 2018. Date of publication August 20, 2018; date of current version February 22, 2019. This work was supported in part by EPSRC under Project EP/Noo4558/1 and Project EP/PO34284/1, and in part by the European Research Council's Advanced Fellow Grant QuantCom. *(Corresponding author: Lajos Hanzo.)*

N. Hosseinidehaj and R. Malaney are with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia.

Z. Babar, S. X. Ng, and L. Hanzo are with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (e-mail: lh@ecs.soton.ac.uk).

Digital Object Identifier 10.1109/COMST.2018.2864557

[1] The superposition of a logical one and zero may be viewed as a coin spinning in a box, where we cannot claim to show its state being 'head' or 'tail'. When we stop spinning the coin, and lift the lid of the box, the superposition-based quantum state collapses back into the classical domain as a consequence of us observing it.

This work is licensed under a Creative Commons Attribution 3.0 License. For more information, see http://creativecommons.org/licenses/by/3.0/

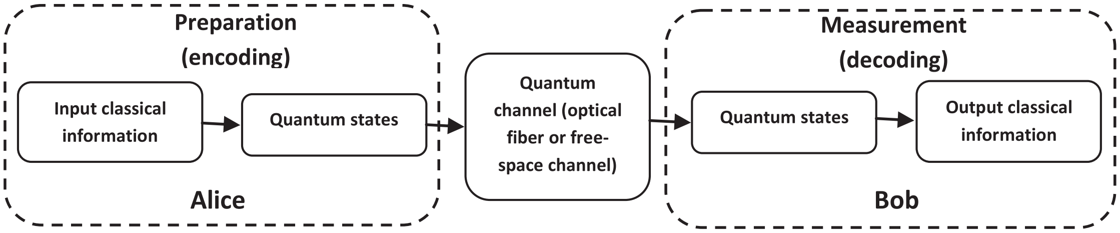

Preparation
(encoding)
Input classical information
Quantum states
Alice
Quantum channel (optical fiber or free-space channel)
Measurement
(decoding)
Quantum states
Output classical information
Bob

Fig. 2. Basic quantum communications schematic for transmitting classical information over a secure quantum channel. **Preparation**: Encoding classical information into quantum states. **Channel**: Secure quantum transmission using optical fiber or free space optical. **Measurement**: Decoding the received quantum states, yielding classical information.

Quantum communication entails the transfer of quantum states from one place to another via a quantum channel. In a generic form, quantum communication consists of three steps: (i) the preparation of quantum states - where the original classical information is encoded into quantum states; (ii) the transmission of the prepared quantum states over a quantum channel such as optical fiber or a free-space optical (FSO) channel - where the states are transmitted from a transmitter, held by Alice, to a receiver, named Bob; and (iii) detection - where the received states are decoded using quantum measurement resulting in some output classical information. A schematic including these three steps is shown in Fig. 2.

A key motivation for quantum communication of Fig. 2 is that the quantum information, mapped for example to the polarization of a photon, can be shared more securely than classical information. The well-known example of this is quantum key distribution (QKD) [3], whose unconditional security has been theoretically proved (classical cryptography schemes are not proved to be secure). We also note the close connection between quantum communication and quantum entanglement. A pair of quantum states are said to be entangled if, for example, changing the polarization of a photon results in an instantaneous polarization change for its entangled pair. Einstein referred to this as a ‘spooky action at a distance.’ Important quantum communication protocols utilizing entangled states include QKD, quantum teleportation [4]–[6], and entanglement swapping (teleportation of entanglement) [7].

In terms of representing the quantum states in quantum communications, discrete-variable (DV) and continuous-variable (CV) descriptions have been used [8], [9]. In the former, information is mapped to discrete features such as the polarization of single photons [3]. The detection of such features would then be realized by single-photon detectors. In DV technology information is mapped to two (or to a finite number of) basis states. The standard unit of DV quantum information in the two basis form is the quantum bit, also known as the ‘qubit.’ In a qubit, information is carried as a superposition of two orthogonal quantum states which can be represented mathematically as:

$$|\psi\rangle = a_1|0\rangle + a_2|1\rangle \tag{1}$$

with $|a_1|^2 + |a_2|^2 = 1$, where the complex numbers a_1 and a_2 can be considered as probability amplitudes. The notation $|.\rangle$ is used to indicate that the object is a vector.[2] Explicitly, the superimposed state of Eq. (1) implies that the qubit concurrently exists in the states $|0\rangle$ and $|1\rangle$. However, it collapses to one of the two states upon measurement. Fig. 3 summarizes the fundamental attributes of qubits, which makes quantum communication absolutely secure.

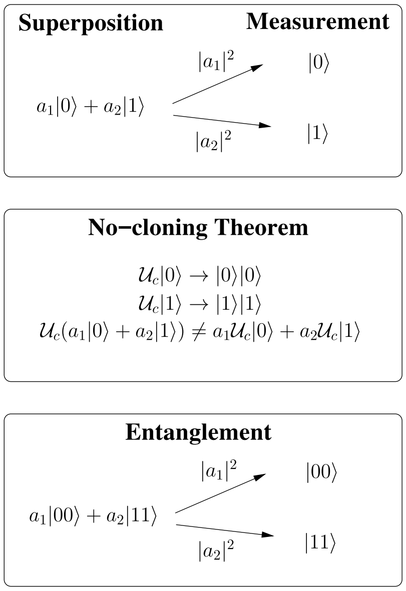

Superposition
Measurement
$|a_1|^2$
$|0\rangle$
$a_1|0\rangle + a_2|1\rangle$
$|a_2|^2$
$|1\rangle$
No−cloning Theorem
$\mathcal{U}_c|0\rangle \rightarrow |0\rangle|0\rangle$
$\mathcal{U}_c|1\rangle \rightarrow |1\rangle|1\rangle$
$\mathcal{U}_c(a_1|0\rangle + a_2|1\rangle) \neq a_1\mathcal{U}_c|0\rangle + a_2\mathcal{U}_c|1\rangle$
Entanglement
$|a_1|^2$
$|00\rangle$
$a_1|00\rangle + a_2|11\rangle$
$|a_2|^2$
$|11\rangle$

Fig. 3. Fundamental characteristics of qubits: (a) **Superposition & Measurement**: A qubit exists in superposition of the states $|0\rangle$ and $|1\rangle$. However, when measured, it collapses to the state $|0\rangle$ with a probability of $|a_1|^2$ and the state $|1\rangle$ with a probability of $|a_2|^2$. Hence, measurement of the qubit perturbs its coherent superposition. (b) **No-cloning Theorem**: An arbitrary quantum state cannot be cloned. Assume a hypothetical cloning operator $\mathcal{U}_c$, it is straightforward to show that cloning of a state $|\psi\rangle$ is not equivalent to cloning the constituent basis states, hence a quantum cloning operator $\mathcal{U}_c$ does not exist. (c) **Entanglement**: Qubits are said to be entangled, if measuring one qubit reveals information on the value of the other. In the example given, if the first qubit is found to be in the state $|0\rangle$ (or $|1\rangle$) upon measurement, then the second qubit also exists in the state $|0\rangle$ (or $|1\rangle$), hence a mysterious relation exists between the two entangled qubits.

As an alternative approach, CV encoding has also been introduced [10], [11], and it is this type of encoding that forms the focus of this work. Such encoding is

[2] Note we have utilised the standard quantum mechanical notation for a vector in a vector space, i.e., $|\psi\rangle$, where ψ is a label for the vector (any label is valid). The entire object $|\psi\rangle$ is sometimes called a ‘ket’. Note also that $\langle\psi|$ is called a ‘bra’ which is the Hermitian conjugate or adjoint of the ket $|\psi\rangle$. In quantum mechanics, bra-ket notation is a standard notation for describing quantum states.

more appropriate for quantum information carriers such as laser light. In CV technology, information is usually encoded onto the quadrature variables of the optical field [10]–[15], which constitute an infinite-dimensional Hilbert space. Detection of these variables is normally realized by high-efficiency homodyne (or heterodyne) detectors, which are capable of operating at a faster transmission rate than single-photon detectors [16]–[18]. The field's quadrature components (representing the quantum state) can be considered as related to the amplitude and phase of the laser light. Hence, CV states can be generated and detected using off-the-shelf state-of-the-art optical hardware [10]–[15]. In quantum mechanics, the quadrature components can also be considered as corresponding to the position and momentum of a harmonic oscillator.

There are generally three quantum communication scenarios, namely, the use of optical fibers, the use of terrestrial FSO channels, and the use of FSO channels to satellites. These scenarios are complementary and all may be expected to play a role in the emerging global quantum communication infrastructure. Fiber technology has the key advantage that once in place, an unperturbed channel from A to B exists. In fact, in fiber links the photon transfer is hardly affected by external conditions such as background light, the weather or other environmental obstructions. However, fiber suffers both from optical attenuation and polarization-preservation problems, which therefore limit its attainable distance to a few hundred kilometers [19]–[30]. These distance limitations may be overcome by the development of suitable quantum repeaters [31]. Losses in fiber are due to inherent random scattering processes, which increase exponentially with the fiber length. Explicitly, the transmissivity determining the fraction of energy received at the output of a fiber link of length L is given by $\tau = 10^{-\alpha_{\text{fiber}} L/10}$, where the value of α_{fiber} is highly dependent on the wavelength. Losses are minimised at the wavelength of 1550 nm, where for silicon fiber $\alpha_{\text{fiber}} \simeq 0.2$ dB/km.

Replacing the fiber channel with a FSO channel has the immediate advantage of lower losses [32]–[35], largely because the atmosphere provides for low absorption. The atmosphere also provides for almost unperturbed propagation of the polarization states. Additionally, FSO channels offer convenient flexibility in terms of infrastructure establishment, with links to moving objects also feasible [36]–[38]. However, terrestrial FSO quantum communications remain ultimately distance-limited, due to (amongst other issues) the curvature of the Earth, potential ground-dwelling line-of-sight (LoS) blockages, as well as atmospheric attenuation and turbulence.

FSO quantum communication via satellites [39]–[69] has the additional advantage that communications can still take place, even when there is no direct free-space LoS from A to B. That is, assuming that LoS paths from a satellite to two ground stations exist, satellite-based FSO communication can still proceed. The range of satellite-based communication is also potentially much larger than that allowed by direct terrestrial FSO connections, since the former circumvents the terrestrial horizon limit and there are lower photonic losses at high altitudes. In satellite-based FSO communications, only a small fraction of the propagation path (less than 10 km) is through the atmosphere - meaning most of the propagation path experiences no absorption and no turbulence-induced losses. The utilisation of satellites also allows for fundamental studies on the impact of relativity on quantum communications [39]. The key disadvantage of satellite-based quantum communications is, however, atmospheric turbulence-induced loss. The above discussions are summarized in Fig. 4.

The quantum communication system of Fig. 4 has given rise to new security paradigms. At the time of writing most of the classical cryptography schemes are based on the Rivest-Shamir-Adleman (RSA) protocol [70] in which the encryption key is public. These cryptography schemes are based on the concept of one-way functions, i.e., on functions which are easy to compute but extremely difficult to invert. Hence, the grade of security of these schemes cannot be irrevocably proved in principle. In fact, the security of these schemes is not unconditional, since they are based on certain computational power assumptions. Thus, if quantum computers were available today with a substantial amount of parallel computational power, RSA cryptography schemes could be broken. However, unconditional security is indeed possible using the so-called one-time pad scheme of [71], where a symmetric, random secret key is shared between the transmitter and receiver. To elaborate, in the one-time pad scheme, the transmitter (Alice) encodes the message by applying modulo addition between the plaintext bits and an equal number of random bits of the shared secret key. At the receiver, Bob decodes the received message by applying the same modulo addition between the received ciphertext and the shared secret key. If Alice and Bob never reuse their key, the one-time pad scheme of [71] cannot be broken, in principle. However, the main problem of this scheme is the generation of the secret key - a key which is as long as the message itself and must be used only once. This problem becomes severe, when a large amount of information has to be securely transmitted. Partially because of this limitation, public-key cryptography is more widely used than the one-time pad scheme. However, QKD, which is based on the laws of quantum physics, allows Alice and Bob to generate secret keys that can later be used to communicate with unconditional information-theoretic security, regardless of any future advances in computational power. Explicitly, the security of QKD is based on some of the fundamental principles of quantum physics. From an attacker's perspective, the ultimate goal is to have a perfect copy of the quantum state sent by Alice to Bob. However, it is impossible to acquire this owing to the no-cloning theorem mentioned in Fig. 3, which states that it is impossible to create an identical copy of an arbitrary unknown quantum state, while keeping the original quantum state intact [72], [73]. This simple, but crucial, observation can be traced back to the fact that quantum mechanics is a linear theory.

Fig. 5 shows the schematic of a QKD system, which can be divided into two main stages. Firstly, a quantum communication part where a pair of distant and trusted parties, Alice and Bob, generate two sets of correlated data through the transmission of a significant number of quantum states over an

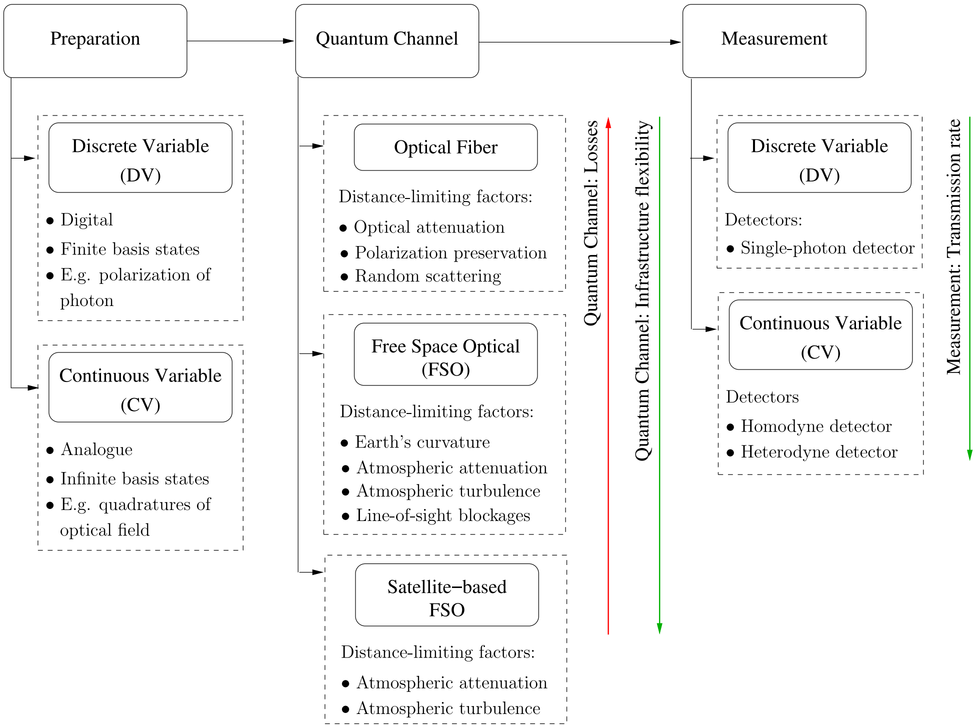


Fig. 4. Insights into the quantum communications system of Fig. 2.

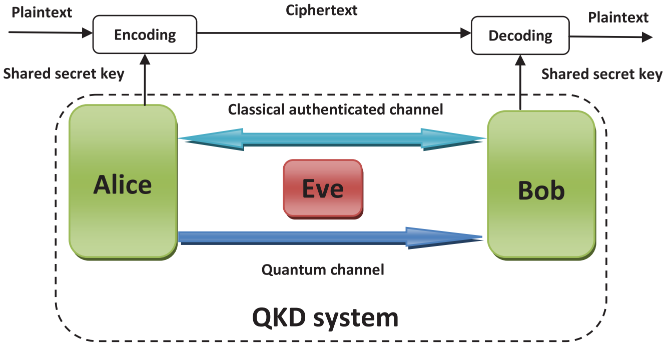


Fig. 5. A schematic of a QKD system: Alice and Bob are connected by a quantum channel, to which Eve has full access without any limitation (other than those constrained by the laws of physics). They are also connected by an authenticated classical channel, which Eve can only monitor. The final shared key between Alice and Bob, which is unconditionally secure, can then be used to transmit (encode and decode) secret messages.

insecure quantum channel.[3] Secondly, by the use of a classical post-processing protocol [74], [75] operated over a public but authenticated (meaning that the transferred data is known to be unaltered) classical channel, Alice and Bob extract from their correlated data a secret key that is unknown to a potential eavesdropper, Eve. The final key, which is unconditionally secure can then be used to transmit secret messages [76], [77]. Note that in QKD the quantum channel is open to any possible manipulation by Eve, which means that Eve has full access to the quantum channel without any computational (classical or quantum) limitation other than those imposed by the laws of quantum physics. However, Eve can only *monitor* the public classical channel, without *modifying* the messages (since the channel is authenticated).

In line with the quantum communication system of Fig. 4, there are two main techniques of implementing QKD, namely DV-QKD and CV-QKD. As the name implies, DV-QKD maps the key information to a single photon's phase or polarization [3], [78], [79], and invokes single-photon detectors. By contrast, CV-QKD maps the key information to the quadrature variables of the optical field and exploits homodyne (or heterodyne) detection [10]–[15], which can be implemented using off-the-shelf optical hardware. Hence, CV-QKD may be viewed as a specialized application of classic optical communications. More precisely, CV-QKD is one of the few quantum applications, which rely on state-of-the-art communications technology, hence ensuring a relatively smooth transition from the classical to the ultra-secure quantum regime. Motivated by this, we set out to survey and characterise the capabilities of CV quantum technology, in particular the family of satellite-based quantum communications solutions, which is essential for realizing our vision of the global quantum communications system encapsulated in Fig. 1. Since CV entanglement has been widely relied upon as a basic resource for CV-QKD [80], our survey is focused on satellite-based CV quantum communication in the context of CV entanglement distribution and its application to CV-QKD. A brief comparison of this survey to other published surveys on topics related to CV quantum communication is presented in Table I, which are mostly targeted towards the specialized quantum fraternity. By contrast, we have adopted a slow-paced tutorial approach for bridging

[3] The term 'insecure' here indicates the presence of an eavesdropper. However, please note that an eavesdropper cannot make a copy of the transmission, since quantum channel is intrinsically protected against copying owing to the no-cloning theorem. An eavesdropper can only 'listen to', or more specifically 'measure', the quantum information.

TABLE I
COMPARISON OF THIS STUDY WITH AVAILABLE SURVEYS

Approach	Satellite-based quantum communication	Atmospheric fading quantum channels	CV quantum systems	Quantum communication protocols	QKD			Gaussian CV quantum communication	Non-Gaussian CV quantum communication	CV quantum teleportation	CV entanglement swapping
					DV-QKD	CV-QKD	Security analysis				
Braunstein and van Loock [9]			✓	✓		✓		✓		✓	✓
Pirandola and Mancini [81], and Pirandola *et al* [82]			✓	✓				✓		✓	✓
Adesso and Illuminati [83]			✓					✓	✓		
Gisin and Thew [84]				✓	✓						
Scarani *et al* [76]			✓	✓	✓	✓	✓	✓			
Andersen *et al* [85]			✓	✓		✓		✓		✓	
Wang *et al* [86]			✓	✓		✓	✓	✓		✓	✓
Weedbrook *et al* [87]			✓	✓		✓	✓	✓		✓	
Lo *et al* [88], and Diamanti *et al* [89]			✓	✓	✓	✓					
Bedington *et al* [40]	✓			✓	✓						
This survey	✓	✓	✓	✓		✓	✓	✓	✓		✓

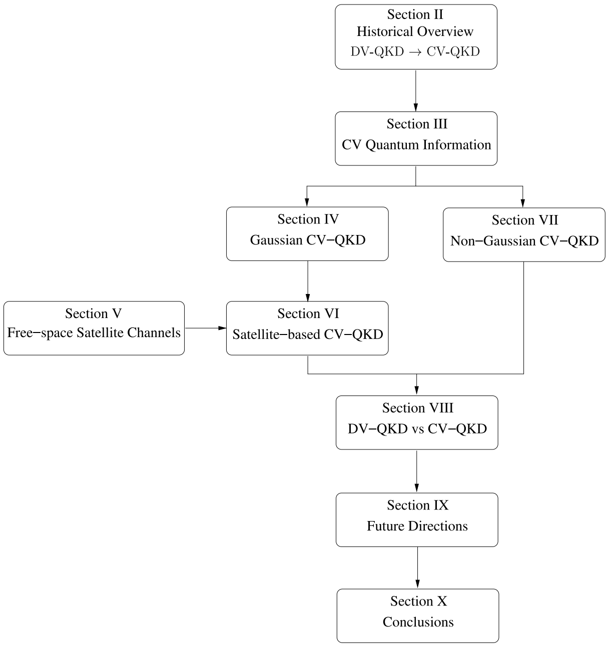


Fig. 6. Paper rationale.

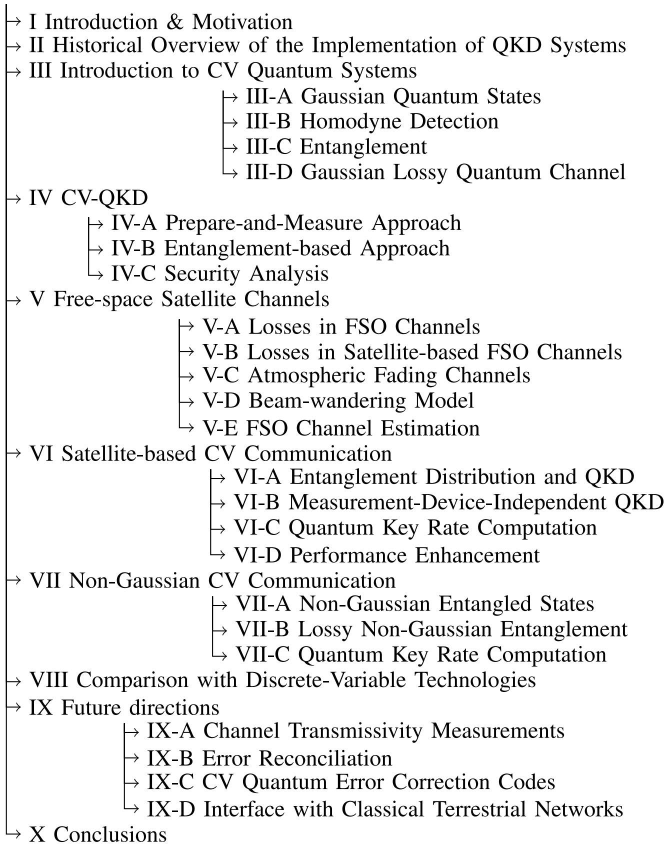
the classical as well as the quantum working groups. For the readers' convenience, the rationale of this paper is captured in Fig. 6, while a detailed paper outline is given in Fig. 7.

II. Historical Overview of the Implementation of Quantum Key Distribution Systems

In this section, we survey the major milestones achieved in the implementation of free-space QKD systems, which are chronologically arranged in Table II.

QKD constitutes the most studied quantum communication protocol, and has been deployed over both fiber and FSO channels. Indeed, the implementation of QKD over optical fibers has already been commercialised [90]–[92]. Terrestrial FSO quantum communications have been successfully deployed over very long distances [32]–[35]. In 2007, entanglement-based QKD and decoy-state QKD were realized over a 144 km FSO link between the Canary Islands of La Palma and Tenerife [78], [79], [93]. In addition to QKD, long-distance terrestrial FSO experiments have also been carried out to implement both entanglement distribution [93], [94] and quantum teleportation [95], [96]. The above long-distance FSO quantum communication experiments have been implemented at night. However, in a recent experiment FSO terrestrial QKD over 53 km has also been demonstrated during the day by choosing an appropriate wavelength, spectrum filtering and spatial filtering [97]. Nonetheless, in both fiber and FSO QKD implementations, the increasing levels of channel attenuation and noise tend to limit the maximum distance of successful key distribution to a few hundred kilometers.

A promising way of extending the deployment range of QKD is through the use of satellites. Indeed, it is widely anticipated that the reliance on satellites will assist in the expansion of quantum communication to global scales [39]–[69]. Full-scale verifications of satellite-based QKD have been reported in [36] (by demonstration of QKD between an aeroplane and a ground station), in [37] (by demonstration of QKD using a moving platform on a turntable, and a floating platform on a hot-air balloon), and in [38] (by demonstration of QKD from a stationary transmitter to a moving receiver platform traveling at an angular speed equivalent to a 600 km altitude satellite). Furthermore, several satellite-based quantum communication projects have been reported in [41]–[46]. In [47]–[49], a



- I Introduction & Motivation
- II Historical Overview of the Implementation of QKD Systems
- III Introduction to CV Quantum Systems
  - III-A Gaussian Quantum States
  - III-B Homodyne Detection
  - III-C Entanglement
  - III-D Gaussian Lossy Quantum Channel
- IV CV-QKD
  - IV-A Prepare-and-Measure Approach
  - IV-B Entanglement-based Approach
  - IV-C Security Analysis
- V Free-space Satellite Channels
  - V-A Losses in FSO Channels
  - V-B Losses in Satellite-based FSO Channels
  - V-C Atmospheric Fading Channels
  - V-D Beam-wandering Model
  - V-E FSO Channel Estimation
- VI Satellite-based CV Communication
  - VI-A Entanglement Distribution and QKD
  - VI-B Measurement-Device-Independent QKD
  - VI-C Quantum Key Rate Computation
  - VI-D Performance Enhancement
- VII Non-Gaussian CV Communication
  - VII-A Non-Gaussian Entangled States
  - VII-B Lossy Non-Gaussian Entanglement
  - VII-C Quantum Key Rate Computation
- VIII Comparison with Discrete-Variable Technologies
- IX Future directions
  - IX-A Channel Transmissivity Measurements
  - IX-B Error Reconciliation
  - IX-C CV Quantum Error Correction Codes
  - IX-D Interface with Classical Terrestrial Networks
- X Conclusions

Fig. 7. Paper structure.

satellite-to-ground single-photon downlink was simulated by reflecting weak laser (coherent) pulses (emitted by the ground-based station) off a low-Earth-orbit (LEO) satellite. In addition to experimental demonstrations, quantum communications with orbiting satellites have also been investigated by a growing number of feasibility studies [39], [50]–[61]. Recently, the in-orbit operation of a photon-pair source aboard a nanosatellite has been reported, which demonstrates photon-pair generation and polarization correlation under space conditions [64].

Quantum communication via satellites has very recently been given an enormous boost with the launch of the world's first quantum satellite, Micius, by China [66]. Building on the previously mentioned experiments, this new LEO satellite creates entangled photon pairs, sending them down to Earth for subsequent processing in a diverse range of communication scenarios. For example, using Micius, satellite-based distribution of entangled photon pairs in the downlink to two terrestrial locations separated by 1203 km has been demonstrated [67]. Quantum teleportation of single-photon qubits from a ground station to Micius through an uplink channel has also been demonstrated [68]. Extensions of this technology to significantly smaller satellites has just been reported for a Japanese micro-satellite and an optical ground station [65].

All of the previous FSO quantum communication systems referred to above have been focussed on DV technologies [32]–[69], [78], [79], [93]–[97]. They are based on single-photon technology and use single-photon detectors. Such detectors are impaired by background light, and involve spatial, spectral and/or temporal filtering in order to reduce this noise [97]. By contrast, in CV quantum communication, homodyne detection (in which the signal field is mixed with a strong coherent laser pulse, called the "local oscillator") is used for determining the field quadratures of light. Homodyne detectors offer better immunity to stray light [16], since the local oscillator is also capable of assisting in both spatial and spectral filtering. Also, such homodyne detectors are more efficient than single-photon detectors, since the p-i-n (PIN) photodiodes used in them offer higher quantum efficiencies than the avalanche photodiodes of single-photon detectors. Hence, CV-QKD can generally be considered to be more robust against background noise than DV-QKD.

In [16] and [98] the feasibility of a point-to-point CV-QKD (with coherent polarization states of light) has been demonstrated over a 100 m FSO link. In [99]–[101] the non-classical properties of CV quantum states propagating through the turbulent atmosphere have been analysed. Gaussian[4] entanglement distribution through a single point-to-point atmospheric channel and its applicability to CV-QKD have been studied in [102]. The entanglement properties of quantum states in the turbulent atmosphere have also been studied in [103] and [104]. Satellite-based CV quantum communication in the context of Gaussian and non-Gaussian entanglement distribution, and its application to CV-QKD, have been investigated in detail in [105]–[109]. The results presented in [105]–[109] apply for both a single point-to-point atmospheric channel, and in combined satellite-based atmospheric channels where the satellite acts as a relay. Recently, a point-to-point CV quantum communication experiment relying on the coherent polarization states of light has been established over a 1.6 km FSO link in an urban environment [110]. The distribution of polarization squeezed states[5] of light through an urban 1.6 km FSO link has also been demonstrated [111]. Recently, an experiment has been carried out relying on homodyne detection at a ground station of optical signals transmitted from a geostationary satellite [112]. This experiment is important in that it clearly demonstrates the feasibility and potential of satellite-based CV-QKD implementations.

III. Introduction to CV Quantum Systems

Any isolated physical system is associated to a Hilbert space, i.e., a complex vector space with inner product. The system is completely described by its state vector, which is a unit vector in the system's Hilbert space.

The simplest quantum mechanical system is a qubit, which has a two-dimensional Hilbert space. Supposing $|0\rangle$ and $|1\rangle$

[4] Gaussian quantum states are CV states with field quadratures exhibiting a Gaussian probability distribution.

[5] In quantum optics, there is an uncertainty relationship for the quadrature components of the light field, stating that the product of the uncertainties in both quadrature components is at least some quantity times Planck's constant. Hence, the uncertainty relationship dictates some lowest possible noise (i.e., uncertainty) amplitudes for the quadrature components of the light. In squeezed light, a further reduction in the noise amplitude of one quadrature component is carried out by squeezing the uncertainty region of that quadrature component, which is at the expense of an increased noise level in the other quadrature component.

TABLE II
MAJOR ACHIEVEMENTS IN THE IMPLEMENTATION OF FREE-SPACE QUANTUM COMMUNICATIONS

Discrete		Continuous
Free-space entanglement distribution over 7.8 km [33] and 13 km [32] in dense urban environment	2005	
10-hr long entanglement-based QKD demonstrated over 1.5 km [34]		
Entanglement-based QKD and decoy-state QKD realized over 144 km [78], [79], [93]		
Long-distance entanglement distribution using terrestrial FSO [93], [94]		Point-to-point CV-QKD over a 100 m FSO link [16], [98]
	2010	
Long-distance teleportation using terrestrial FSO [95], [96]		
Full-scale verification of satellite-based QKD [36]–[38]		
		Point-to-point CV quantum communication over a 1.6 km FSO link in urban environment [110], [111]
	2015	
Day-time FSO terrestrial QKD over 53 km [97], World's first quantum satellite Micius launched [66], Satellite-based entanglement distribution using Micius over 1203 km [67], Teleportation using Micius over 1400 km [68], quantum transmission using a 48-kg micro-satellite [65]		Homodyne detection using a geostationary satellite demonstrating the feasibility of satellite-based CV-QKD [112]

form an orthonormal[6] basis for this Hilbert space, an arbitrary state vector in the Hilbert space can be written as $|\psi\rangle = a_1|0\rangle + a_2|1\rangle$, where a_1 and a_2 are complex numbers. The normalization condition for state vectors (or the condition that $|\psi\rangle$ be a unit vector), $\langle\psi|\psi\rangle = 1$, is equivalent to $|a_1|^2 + |a_1|^2 = 1$.[7] When we measure a qubit in the basis $\{|0\rangle, |1\rangle\}$ we obtain either the result $|0\rangle$, with probability $|a_1|^2$, or the result $|1\rangle$, with probability $|a_2|^2$.

Now we can extend a two-dimensional Hilbert state to an arbitrary-dimensional Hilbert state (even infinite-dimensional). A quantum state with finite-dimensional Hilbert space is called discrete-variable quantum state, and a quantum state with infinite-dimensional Hilbert space is called continuous-variable quantum state. In an arbitrary-dimensional Hilbert space the arbitrary quantum state $|\psi\rangle$ can be expanded in an arbitrary orthonormal basis as $|\psi\rangle = \sum_i \psi_i|v_i\rangle$, where the complex number ψ_i is $\psi_i = \langle v_i|\psi\rangle$. By definition the basis is complete (i.e., $\sum_j |v_j\rangle\langle v_j| = I$, with I the identity operator) and orthonormal (i.e., $\langle v_i|v_j\rangle = \delta_{ij}$).

Now let us consider the quantum measurement of an arbitrary quantum state $|\psi\rangle$. Quantum measurements are described by operators[8] $\hat{M}_m$, where the index *m* refers to the measurement result. Note that the measurement operators satisfy the completeness equation $\sum_m \hat{M}_m^\dagger \hat{M}_m = I$. Considering the initial quantum state $|\psi\rangle$, the probability that outcome *m* occurs as a result of the quantum measurement $\hat{M}_m$ upon the state $|\psi\rangle$ is given by $p_m = \langle\psi|\hat{M}_m^\dagger \hat{M}_m|\psi\rangle$, and the state of the system after the measurement collapses onto $\frac{1}{\sqrt{p_m}}\hat{M}_m|\psi\rangle$. Due to the completeness of the measurement operators we have $\sum_m p_m = 1$.

A projective measurement is described by an observable $\hat{M}$. Each observable quantity is associated with a Hermitian operator whose eigenvalues correspond to the possible values of the observable. The observable has a spectral decomposition $\hat{M} = \sum_m \lambda_m \hat{P}_m$, where $\hat{P}_m = |u_m\rangle\langle u_m|$. The vectors $|u_m\rangle$ are the orthonormal set of eigenvectors of the observable $\hat{M}$ with real-valued eigenvalues λ_m which satisfy $\sum_m |u_m\rangle\langle u_m| = I$. The probability for obtaining the measurement result λ_m upon measuring the state $|\psi\rangle$ is given by $p_m = |\langle u_m|\psi\rangle|^2$. Hence, the probability p_m is determined by the size of the component of $|\psi\rangle$ in direction of the eigenvector $|u_m\rangle$. When the measurement result λ_m is obtained, the quantum state $|\psi\rangle$ collapses onto $\frac{1}{\sqrt{p_m}}\hat{P}_m|\psi\rangle$.

One form of a CV quantum system is that represented by N bosonic modes, such as those corresponding to N quantized radiation modes of the electromagnetic field [9], [83], [85]–[87], [113], [114]. A single photon has four degrees of freedom, helicity (polarization) and the three components of the momentum vector. In principle, quantum information can be encoded into any one of these degrees of freedom. A single 'mode' of an electromagnetic field refers to a specific combination of these photonic degrees of freedom. In many circumstances different modes can be simply represented by different frequencies (since frequency is related to momentum). For a beam of photons, the *number* of photons in the beam constitutes another means to encode quantum information. Quantum information encoded into the quadratures of the electromagnetic field (formally defined below) are related to an encoding in this additional degree of freedom. Since the quadrature operators have continuous spectra, we can describe the values of such operators as CV variables.

A single mode of a CV system can be described as a single quantum harmonic oscillator of a specific frequency, where the electric and magnetic fields play the 'roles' of the position and momentum [115]. It will be useful to further illustrate this concept. Consider the case of a single-frequency radiation field confined to a one-dimensional cavity with walls that are perfectly conducting. Assume the z-axis is parallel to the length of the cavity and the cavity walls are located at $z = 0$ and $z = L$. The electric field within the cavity will form a standing wave. Without loss of generality, we can take the electric field to be polarized perpendicular to the z-axis, and in the positive x-direction (we take the x and z coordinates to

[6] A set of vectors $|i\rangle$ is orthonormal if each vector is a unit vector, and distinct vectors are orthogonal, i.e., $\langle i|j\rangle = \delta_{ij}$, where δ_{ij} is the Kronecker delta function.

[7] Note that the overlap $\langle\varphi|\psi\rangle$ indicates the inner product between the vectors $|\psi\rangle$ and $\langle\varphi|$ (the adjoint of the vector $|\varphi\rangle$) in the Hilbert space.

[8] The operator serves as a linear function which acts on the states of the system. While quantum states correspond to vectors in a Hilbert space, operators can be regarded as matrices.

be in same plane and the *y* plane perpendicular to the *x* plane). In terms of the distance vector *r* and time *t*, the electric field can then be written as $E(r,t) = e_x E_x(z,t)$, where e_x is a unit-length polarization vector. Given our boundary conditions, and assuming a radiation source-free cavity, the electric field satisfying Maxwell's equations can be written as [115]

$$E_x(z,t) = \sqrt{\left(\frac{2\omega^2}{V_o\varepsilon_0}\right)} \quad q(t)\sin(kz), \tag{2}$$

where $k = \omega/c$ is the wave number (ω is the frequency of the mode and *c* is the speed of light in vacuum), ε_0 is the vacuum permittivity, *q*(*t*) is a time-dependent factor having the dimension of length (meters), and V_o is the effective volume of the cavity.[9] For the present purposes we will assume the frequency is one of those allowed by the boundary conditions, namely, $\omega_n = c(n\pi/L)$, where $n = 1, 2, \ldots$.

Similarly, the magnetic field can be written $B(r,t) = e_y B_y(z,t)$, where e_y is a unit-length polarization vector, and [115]

$$B_y(z,t) = \frac{\mu_0\varepsilon_0}{k}\sqrt{\left(\frac{2\omega^2}{V_o\varepsilon_0}\right)}\, p(t)\cos(kz). \tag{3}$$

Here $p(t) = \dot{q}(t)$, where the dot denotes the time derivative, and μ_0 is the vacuum permeability. Based on these equations it is then straightforward to show that the Hamiltonian, H_o, of the electromagnetic field can be written as [115]

$$H_o = \frac{1}{2}\int dV_o\left(\varepsilon_0 E_x^2(z,t) + \frac{1}{\mu_0}B_y^2(z,t)\right). \tag{4}$$

Substituting $E_x(z,t)$ and $B_y(z,t)$ in H_o from Eq. (2) and Eq. (3) respectively and exploiting that $\sin^2(\frac{\omega}{c}z) + \cos^2(\frac{\omega}{c}z) = 1$ the Hamiltonian of the single-mode electromagnetic field can be written as

$$H_o = \frac{1}{2}\left(p^2 + (\omega q)^2\right). \tag{5}$$

This equation can be compared with the Hamiltonian of the classical harmonic oscillator for a particle of mass *m* viz., $H_o = \frac{1}{2}(p^2/m + (m\omega q)^2)$, where we have taken the generalised coordinate $q = x$ and set $p = m\dot{x}$, *x* being the position. Comparing these two Hamiltonians, it can be seen that a single-mode electromagnetic field is formally equivalent to a harmonic oscillator of unity mass, where the electric and magnetic fields play roles similar to that of the position and momentum of a particle.[10]

In quantum systems we replace variables, such as *q*, *p*, *E*, *B* and *H* of the classical system, by their corresponding operator[11] equivalents, e.g., $\hat{q}$, $\hat{p}$, $\hat{E}$, $\hat{B}$ and $\hat{H}$. Then the Hamiltonian of the single-mode electromagnetic field becomes $\hat{H}_o = \frac{1}{2}(\hat{p}^2 + (\omega\hat{q})^2)$. As such, we can now see how a single mode of a CV system can indeed be described as a single quantum harmonic oscillator. Furthermore, note that the operators $\hat{q}$ and $\hat{p}$ are Hermitian (or self-adjoint). In quantum physics Hermitian operators correspond to observable quantities, where an observable is an operator that corresponds to a physical quantity, such as position or momentum, that can be measured.

However, it will be useful to introduce non-Hermitian operators $\hat{a}$ (the annihilation operator) and $\hat{a}^\dagger$ (the creation operator). These can be written as,

$$\hat{a} = (2\hbar\omega)^{(-1/2)}(\omega\hat{q} + i\hat{p}), \tag{6}$$

$$\hat{a}^\dagger = (2\hbar\omega)^{(-1/2)}(\omega\hat{q} - i\hat{p}), \tag{7}$$

where $\hbar = h/2\pi$, with *h* being Planck's constant. These bosonic field operators satisfy the commutation relation $[\hat{a}, \hat{a}^\dagger] = 1$, where the commutator between two operators $\hat{x}$ and $\hat{y}$ is defined to be $[\hat{x}, \hat{y}] = \hat{x}\hat{y} - \hat{y}\hat{x}$. Note that since the annihilation and creation operators are non-Hermitian, they correspond to *non-observable* quantities.

It can be easily shown that our new non-Hermitian operators have a time dependence, under free evolution, which can be expressed as $\hat{a} = \hat{a}(0)\exp(-i\omega t)$ and $\hat{a}^\dagger = \hat{a}^\dagger(0)\exp(i\omega t)$. As such, the electric field operator can then be re-written as

$$\hat{E_x}(z,t) = \sqrt{\left(\frac{\hbar\omega}{V_0\varepsilon_0}\right)}\sin(kz)\Big[\hat{a}\exp(-i\omega t) + \hat{a}^\dagger\exp(i\omega t)\Big]. \tag{8}$$

Removing the time dependence in the creation and annihilation operators by re-setting $\hat{a} = \hat{a}(0)$ and $\hat{a}^\dagger = \hat{a}^\dagger(0)$, we can in turn define the *quadrature operators* (see later discussion on the freedom to choose the specific form of these)

$$\hat{X}_1 = \frac{1}{2}\left(\hat{a} + \hat{a}^\dagger\right), \tag{9}$$

$$\hat{X}_2 = \frac{1}{2i}\left(\hat{a} - \hat{a}^\dagger\right). \tag{10}$$

In terms of the quadrature operators we can then re-write $\hat{E_x}(z,t)$ as

$$\hat{E_x}(z,t) = 2\sqrt{\left(\frac{\hbar\omega}{V_0\varepsilon_0}\right)}\sin(kz)\Big[\hat{X}_1\cos(\omega t) + \hat{X}_2\sin(\omega t)\Big]. \tag{11}$$

As such, we can see that the quadratures $\hat{X}_1$ and $\hat{X}_2$ can be considered as the amplitudes of the electric field's time-dependent cos and sin components, respectively. Clearly, these components are 90° out of phase with each other - hence the name, quadratures. The quadratures satisfy the commutation relation $[\hat{X}_1, \hat{X}_2] = i/2$.[12]

A CV system of *N* modes follows a similar description to that we have just given for a single mode, except of course the Hilbert space containing the multimode system is larger. The *N*-mode system may be described by a Hilbert space given by the tensor product $\mathcal{H} = \otimes_{k=1}^{N}\mathcal{H}_k$, where $\mathcal{H}_k$ is a single-mode Hilbert space associated with the *k*-th mode. The

[9] To apply this formalism to the free field we calculate the physical observables we are interested in and then simply take the limit $V_0 \to \infty$.

[10] We emphasize that the terms 'position' and 'momentum' here simply refer to the similar roles played by the field quadratures and position and momentum of a particle - e.g., the 'position quadrature' does not in any manner refer to the position of a photon.

[11] Note that operators can be regarded as matrices. In fact, the operator and matrix viewpoints turn out to be completely equivalent [8].

[12] This can be derived from the constraint imposed by quantum mechanics that $[\hat{q}, \hat{p}] = i\hbar$. Note, that in contrast to classical physics where any two observables commute, i.e., their commutator is zero (which means it is possible to know precisely the value of both observables at the same time), in quantum mechanics the quadrature observables of the electromagnetic field do not commute.

creation and annihilation operators for each mode then satisfy the commutation relationships

$$[\hat{a}_k, \hat{a}_{k'}] = \left[\hat{a}_k^\dagger, \hat{a}_{k'}^\dagger\right] = 0, \quad \left[\hat{a}_k, \hat{a}_{k'}^\dagger\right] = \delta_{kk'}, \tag{12}$$

where $\delta_{kk'}$ is the Kronecker delta function.

Consider again the single-mode Hilbert space $\mathcal{H}_k$. This is spanned by the Fock, or number-state basis, $\{|n\rangle_k\}_{n=0}^{\infty}$, where the Fock state $|n\rangle_k$ is the eigenstate of the number operator $\hat{n}_k = \hat{a}_k^\dagger \hat{a}_k$, i.e., $\hat{n}_k|n\rangle_k = n|n\rangle_k$. Put simply, $|n\rangle_k$ represents the state of the electromagnetic field containing exactly *n* photons (quanta) of frequency ω_k. Note that for each mode *k* there exists a *vacuum* state which contains *no* quanta of the field, namely, $|0\rangle_k$, satisfying $\hat{a}_k|0\rangle_k = 0$. The action of the bosonic field operators over the Fock states is given by [9], [87]

$$\hat{a}_k|n\rangle_k = \sqrt{n}|n-1\rangle_k, \quad \hat{a}_k^\dagger|n\rangle_k = \sqrt{n+1}|n+1\rangle_k. \tag{13}$$

Having now formally defined the vacuum state, it is probably useful to note for the unwary that some *apparent* inconsistency lies lurking in the literature (including the many references of this work). This applies to both the constant value applied to $\hbar$, as well as the nomenclature itself. We note that our quadrature operators, as defined thus far, can be used to form $\hat{q} = \sqrt{2\hbar/\omega}\hat{X}_1$ and $\hat{p} = \sqrt{2\hbar\omega}\hat{X}_2$; from which we can easily show consistency with $[\hat{q}, \hat{p}] = i\hbar$. In many works we will find that $\hat{q}$ and $\hat{p}$ written in this form (and also in 'dimensionless' form with, say, $\hbar = \omega = 1$) are also referred to as the 'quadratures.' Also, in many works the cofactor of 1/2 in front of our definitions of $\hat{X}_1$ and $\hat{X}_2$ is replaced by some other constant, e.g., $1/\sqrt{2}$ or 1-allowable re-definitions of course. It is straightforward to determine the vacuum expectation value for any well-defined operator (or function of that operator), e.g., $\langle 0|\hat{X}_1^2|0\rangle = 1/4$, and $\langle 0|\hat{q}^2|0\rangle = \hbar/(2\omega)$. It is common to set $\hbar$ to some numerical constant, usually 1/2, 1 or 2. However, no consistency exists in the literature on this either. Setting $\hbar = 2$ has the convenience of setting the vacuum-state variance of the $\hat{q}$ and $\hat{p}$ operators to 1 (when ω is set to unity).[13]

Bearing in mind the above discussion of inconsistency in nomenclature, we adopt henceforth that $\hbar = 2$ and $\omega = 1$ (unless stipulated otherwise). We also redefine the 'quadrature' operators to be $\hat{q}_k$ and $\hat{p}_k$, now given by the simpler form $\hat{q}_k = \hat{a}_k + \hat{a}_k^\dagger$ and $\hat{p}_k = i(\hat{a}_k^\dagger - \hat{a}_k)$. This will make the notation to follow less cluttered.

Defining the vector of quadrature operators for *N* modes as $\hat{R} = (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_N, \hat{p}_N)$, the commutation relationship between the quadrature operators can be written as $[\hat{R}_i, \hat{R}_j] = 2i\Omega_{ij}$, where $\hat{R}_i$ ($\hat{R}_j$) is the *i*-th (*j*-th) element of the vector $\hat{R}$, and Ω_{ij} is the element of the matrix

$$\mathbf{\Omega} = \bigoplus_{k=1}^{N} \mathbf{\Omega}_0, \ \mathbf{\Omega}_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{14}$$

Since a Hermitian operator has an orthogonal set of eigenvectors with real-valued eigenvalues, the quadrature operator $\hat{q}$ ($\hat{p}$) (which is Hermitian) is an observable with continuous eigenspectra, i.e., $\hat{q}|q\rangle = q|q\rangle$ ($\hat{p}|p\rangle = p|p\rangle$), with orthogonal eigenvectors or eigenstates $|q\rangle$ ($|p\rangle$) having continuous eigenvalues $q\in\mathbb{R}$ ($p\in\mathbb{R}$). Note that the two sets of eigenstates $|q\rangle$ and $|p\rangle$ identify two different bases (i.e., two different sets of orthogonal and complete eigenstates), and each set constitutes a common basis for CV quantum information. A CV quantum state can be defined as a continuous-valued superposition of the field's eigenstates.

All the physical information about a quantum system is contained in its quantum state, represented by a density operator $\hat{\rho}$, which is a trace-one positive operator. A pure quantum state (i.e., the state of an isolated physical system which does not have any interaction with the environment) is described by a unit vector $|\psi\rangle$ in Hilbert space, and its density operator is given by $\hat{\rho} = |\psi\rangle\langle\psi|$.

Unlike pure states, mixed states cannot be described by a single vector in the Hilbert space, because the knowledge about the state preparation is incomplete. In fact, a mixed state is a statistical mixture of pure states, and is described by its associated density operator. The density operator describing a mixed state is in the form of $\hat{\rho} = \sum_i p_i|\psi_i\rangle\langle\psi_i|$, where the pure quantum state $|\psi_i\rangle$ in which the system is prepared occurs with probability p_i. A quantum state $\hat{\rho}$ is said to be a pure state, when we have $\hat{\rho}^2 = \hat{\rho}$. In fact, for pure states we have $\mathrm{Tr}(\hat{\rho}^2) = 1$, and for mixed states we have $\mathrm{Tr}(\hat{\rho}^2) < 1$, where Tr denotes trace.

For a general mixed quantum state $\hat{\rho} = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ the mean value of the observable $\hat{M}$ is given by $\langle\hat{M}\rangle = \sum_i p_i\langle\psi_i|\hat{M}|\psi_i\rangle = \mathrm{Tr}(\hat{\rho}\hat{M})$, where $\langle.\rangle$ denotes the mean value, and the variance of the observable $\hat{M}$ is given by $V(\hat{M}) = \langle\hat{M}^2\rangle - \langle\hat{M}\rangle^2$, where $V(.)$ is the variance. Note that the fluctuations in the quadrature operators (i.e., $\hat{q}$ and $\hat{p}$) of the electromagnetic field can be characterized by the variance of these observables, or by the standard deviation (i.e., the square root of the variance) of these observables denoted by $\Delta(.)$, which is sometimes referred to as the uncertainty of the quadrature operators. Note also that for non-commuting operators $\hat{A}$ and $\hat{B}$ where $[\hat{A}, \hat{B}] = \hat{C}$, we have $\Delta(\hat{A})\Delta(\hat{B}) \geq \frac{1}{2}|\langle\hat{C}\rangle|$. Since the quadrature operators of the electromagnetic field do not commute ($[\hat{q}, \hat{p}] = i\hbar$), there exists an uncertainty relation for the uncertainty of the quadrature operators, called the Heisenberg uncertainty principle. In a *N*-mode CV system the Heisenberg uncertainty principle is defined for the quadrature operators of each mode *k*, and is given by $V(\hat{q}_k)V(\hat{p}_k) \geq 1$ (recall again $\hbar = 2$). According to the uncertainty principle if we prepare a large number of quantum systems in identical states, and then measure the quadrature $\hat{q}$ of some of those states, and measure the quadrature $\hat{p}$ of others, then the variance of the $\hat{q}$ results times the variance of the $\hat{p}$ is at least one. Note again, that the quadrature variance of the vacuum state of a single mode is one, i.e., we have $V(\hat{q}) = V(\hat{p}) = 1$, which is the lowest possible variance reachable symmetrically by the $\hat{q}$ and $\hat{p}$ quadratures according to the uncertainty relationship.

A quantum state $\hat{\rho}$ of a *N*-mode CV system can also be described in terms of a characteristic function $\chi_c(\xi) = \mathrm{Tr}(\hat{\rho}\hat{\mathrm{D}}(\xi))$, where $\hat{D}(\xi) = \exp(i\hat{R}\mathbf{\Omega}\xi)$ is the Weyl operator [9], [87], and $\xi \in \mathbb{R}^{2N}$. The quantum state $\hat{\rho}$ can also be

[13] Note the variance of $\hat{q}$ in the vacuum state is just $\langle 0|\hat{q}^2|0\rangle$ since the vacuum expectation of $\hat{q}$ is zero (variance $= \langle 0|\hat{q}^2|0\rangle - \langle 0|\hat{q}|0\rangle^2$). Similar is the case for $\hat{p}$.

described in terms of a Wigner function (quasi-probability distribution), which is given by the Fourier transform of the characteristic function χ_c as [9], [87]

$$W(R) = \int_{\mathbb{R}^{2N}} \frac{d^{2N}\xi}{(2\pi)^{2N}} \exp(-iR\boldsymbol{\Omega}\xi)\chi_c(\xi), \tag{15}$$

where $R = (q_1, p_1, \ldots, q_N, p_N)$ is the vector of quadrature variables, with the real-valued variables q and p being the eigenvalues of the quadrature operators. Note that for a single-mode quantum state the probability distribution of a quadrature measurement (marginal distribution) is obtained from the Wigner function of the quantum state by integration over the conjugate quadrature.

The CV quantum states can be visualized using their Wigner function in a phase-space representation, where the axes are defined by a pair of conjugate quadrature variables q and p. In such a phase space, a classical optical field is represented by a single point corresponding to its complex-valued field amplitude. However, the quantum states of light cannot be represented by a single point, since conjugate quadrature variables cannot be measured simultaneously with arbitrary precision due to the Heisenberg uncertainty relationship. Hence the Wigner function is utilized to represent the quantum states in the phase space [9], [85]–[87].

A. Gaussian Quantum States

Gaussian quantum states (for a detailed review, see [86], [87], [114]) are completely characterized by the first moment (or the mean value) of the quadrature operators $\langle \hat{R} \rangle$ and a covariance matrix $\boldsymbol{M}$, i.e., a matrix of the second moments of the quadrature operators defined as

$$M_{ij} = \frac{1}{2}\langle \hat{R}_i\hat{R}_j + \hat{R}_j\hat{R}_i\rangle - \langle \hat{R}_i\rangle\langle \hat{R}_j\rangle. \tag{16}$$

The covariance matrix of a N-mode quantum state is a ($2N \times 2N$) real symmetric matrix, which must satisfy the uncertainty principle, *viz.*, $\boldsymbol{M} + i\boldsymbol{\Omega} \geq 0$. By definition, a Gaussian state having N modes is a CV state whose Wigner function is a Gaussian distribution of the quadrature variables given by

$$W(R) = \frac{\exp\Big(-\frac{1}{2}(R - \langle R\rangle)\, \boldsymbol{M}^{-1}\, (R - \langle R\rangle)^T\Big)}{(2\pi)^N \sqrt{\det(\boldsymbol{M})}}. \tag{17}$$

Some important examples of Gaussian states are vacuum states [9], [86], [87], [115], coherent states [9], [86], [87], [115], thermal states [9], [86], [87], [115] and squeezed states [9], [86], [87], [115]. We discuss some of these Gaussian states further.

1) Vacuum State: The Wigner function of the vacuum state with respect to the conjugate quadrature variables q and p is shown in Fig. 8(a), in which the Wigner function is centered at (0, 0), which means that the vacuum state has a zero mean. The covariance matrix of the vacuum state is the identity matrix, which means that a vacuum state has a symmetric distribution of the quadrature components (see Fig. 8(a)) with both the quadrature components having noise variance of one. This noise is usually termed the vacuum noise or quantum shot noise.

2) Coherent State: A coherent state is generated by applying the displacement operator $\hat{D}$ to the vacuum state formulated as $|\alpha\rangle = \hat{D}(\alpha)|0\rangle$, where $\hat{D}(\alpha) = \exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a})$ is the displacement operator and $\alpha = (q + ip)/2$ is the complex amplitude. Since the displacement operator does not change the variance of the quadratures, coherent states - similarly to vacuum states - exhibit the lowest possible variance reachable symmetrically by the $\hat{q}$ and $\hat{p}$ quadratures. The coherent state is the eigenstate of the annihilation operator, which is formulated as $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$. To elaborate a little further, this state has a mean value of $\langle \hat{R}\rangle = (q, p)$, and the covariance matrix is equal to the identity matrix, which means that a coherent state has a symmetric distribution of the quadrature components with both the quadrature components having noise variance equal to one. This symmetric distribution can be seen in Fig. 8(b), where the Wigner function of the coherent state with a mean value of (3, 5) (which is the centre of the Wigner function) is shown with respect to the conjugate quadrature variables q and p. Note that coherent states are much easier to generate in the laboratory than any other Gaussian state. For example, the laser field is in a coherent state. As an important application in the context of quantum communication, coherent states are used to distribute secret keys in Gaussian CV-QKD protocols [13], [14], [116], [117].

3) Thermal State: Thermal states can be described as a mixture of coherent states. The thermal state has a zero mean and a covariance matrix $\boldsymbol{M_{th}} = v_t\boldsymbol{I}$ associated with $v_t = 2\bar{n} + 1$, where v_t is the noise variance of each quadrature component, $\bar{n}$ >0 is the average number of photons and $\boldsymbol{I}$ is the (2×2)-element identity matrix. This form of the covariance matrix means that a thermal state has a symmetric distribution of the quadrature components, which can be seen in Fig. 8(c) where the Wigner function of the thermal state with $v_t = 5$ is shown with respect to the conjugate quadrature variables q and p. Note that in the generic form of quantum communication the quantum noise of the channel is in a thermal state, called thermal noise.

4) Single-Mode Squeezed Vacuum State: According to the Heisenberg uncertainty relationship, the lowest possible variance reachable symmetrically by the $\hat{q}$ and $\hat{p}$ quadratures is one, i.e., the noise variance of the vacuum state. A reduction in the variance of the $\hat{q}$ (or $\hat{p}$) quadrature below the vacuum noise is possible by *squeezing*. In squeezing, the variance of one continuous variable is in fact decreased below the vacuum noise, while the variance of the conjugate variable is increased. For instance, in a $\hat{q}$-squeezed light, the variance of the $\hat{q}$ quadrature is reduced below the vacuum noise, while the variance of the $\hat{p}$ quadrature is increased above the vacuum noise. A single-mode squeezed vacuum state is generated by applying the single-mode squeezing operator of $\hat{S}_s(r_s) = \exp[r_s(\hat{a}^2 - \hat{a}^{\dagger 2})/2]$ [9], [86], [87], [115] to the vacuum state, where $r_s \in [0, \infty)$ represents the single-mode squeezing parameter.[14] Such a squeezed state has zero mean and a covariance matrix of $\boldsymbol{M} = diag[\exp(-2r_s), \exp(2r_s)]$

[14] Note, in general, squeezing parameters are complex numbers. For simplicity (and to be consistent with most of the literature) we limit them here to real numbers.

when the quantum fluctuations of the $\hat{q}$ quadrature have been squeezed. In this case for the single-mode squeezing represented by r_s >0 we have $V(\hat{q}) < 1$ and $V(\hat{p})$ >1. This means that a single-mode squeezed state does not have a symmetric distribution of the quadrature components, since the variance of one of the quadratures is reduced by squeezing at the expense of an increase in the variance of the conjugate quadrature by the counterpart operation of anti-squeezing. Note, the state still obeys the Heisenberg uncertainty relationship. Such an asymmetric distribution of quadrature components can be seen in Fig. 8(d), where the Wigner function of the single-mode squeezed vacuum state with $r_s = 0.5$ is shown. Here, the $\hat{q}$ quadrature is squeezed. In terms of applications in quantum communications, single-mode squeezed vacuum states are also utilized to distribute secret keys in Gaussian CV-QKD protocols [12], [118]. Note that for $r_s = 0$, the single-mode squeezed state corresponds to the vacuum state.

5) Two-Mode Squeezed Vacuum State: A two-mode squeezed vacuum (TMSV) state is generated by applying the two-mode squeezing operator of $\hat{S}_t(r) = \exp\left[r(\hat{a}_1\hat{a}_2 - \hat{a}_1^\dagger\hat{a}_2^\dagger)/2\right]$ [9], [86], [87], [115] to a pair of vacuum states $|0\rangle|0\rangle$, where $r \in \mathbb{R}$ is the two-mode squeezing parameter, and the indices 1 and 2 represent the two modes. A TMSV state is described in the Fock basis as [9], [86], [87], [115]

$$|\mathrm{TMSV}\rangle = \sum_{n=0}^{\infty} q_n |n\rangle_1 |n\rangle_2, \text{ where}$$
$$q_n = \sqrt{1-\lambda^2}\,\lambda^n, \tag{18}$$

and λ = tanh(r). The two-mode squeezing in dB is given by $-10\log_{10}[\exp(-2r)]$. Such a squeezed state has a zero mean, and a covariance matrix in the following form [9], [86], [87], [115]

$$\boldsymbol{M} = \begin{pmatrix} v\,\boldsymbol{I} & \sqrt{v^2-1}\,\boldsymbol{Z} \\ \sqrt{v^2-1}\,\boldsymbol{Z} & v\,\boldsymbol{I} \end{pmatrix}, \tag{19}$$

where v = cosh (2r) is the quadrature variance of each mode, and **Z** = *diag*(1, −1). Note that the two-mode squeezing operator $\hat{S}_t$ cannot be factorised into the product of the two single-mode squeezing operators $\hat{S}_s$. Hence, the TMSV state is not a product of the two single-mode squeezed vacuum states. In fact, the squeezing (anti-squeezing) operation applied to the quantum fluctuations does not squeeze (anti-squeeze) the variance of the individual modes, but rather that of the superposition of the two modes, so that we have $V(\hat{q}_-) = V(\hat{p}_+) = \exp(-2r)$ and $V(\hat{q}_+) = V(\hat{p}_-) = \exp(2r)$, where $\hat{q}_- = (\hat{q}_1 - \hat{q}_2)/\sqrt{2}$, $\hat{p}_+ = (\hat{p}_1 + \hat{p}_2)/\sqrt{2}$, $\hat{q}_+ = (\hat{q}_1 + \hat{q}_2)/\sqrt{2}$, and $\hat{p}_- = (\hat{p}_1 - \hat{p}_2)/\sqrt{2}$. For a two-mode squeezing operation with r>0, we have $V(\hat{q}_-) = V(\hat{p}_+) < 1$ and $V(\hat{q}_+) = V(\hat{p}_-) > 1$. The correlations between the quadratures of the two modes are known as Einstein-Podolski-Rosen (EPR) correlations, which indicate the presence of bipartite entanglement. Hence, for the two-mode squeezing operation with r>0 the two modes are entangled, where the entanglement increases upon increasing r. The TMSV state associated with r>0 is the most commonly used Gaussian entangled state [9], [83], [86], [87], [113], [114]. In the limit of $r \to \infty$ we have a maximally entangled state having perfect correlations, yielding $\hat{q}_1 = \hat{q}_2$ and $\hat{p}_1 = -\hat{p}_2$. Note that for $r = 0$ the TMSV state corresponds to two (non-entangled) vacuum states.

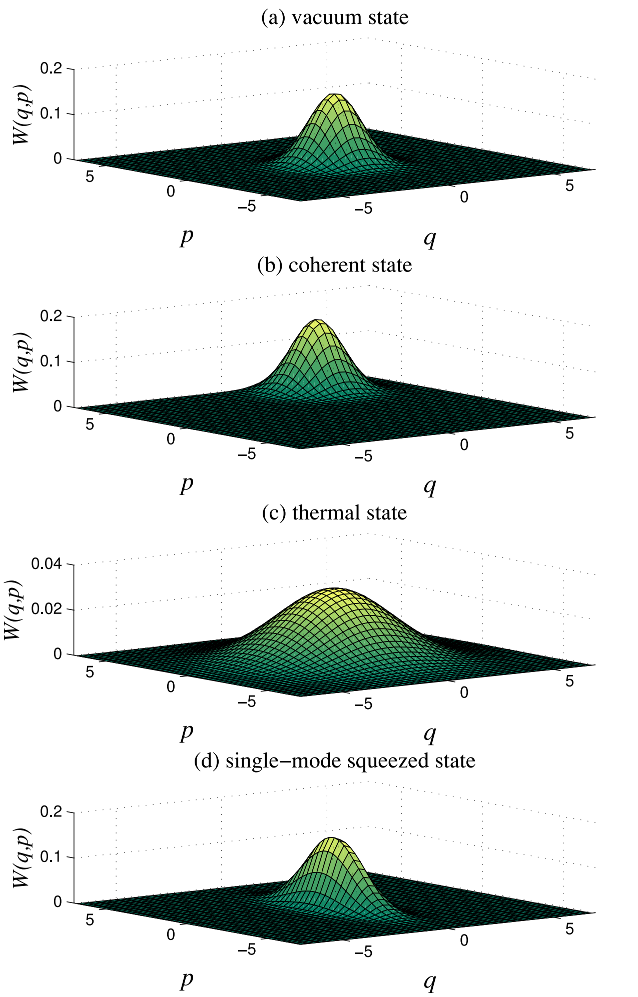


Fig. 8. The Wigner function of the important single-mode Gaussian states including vacuum state, coherent state with a mean value of (3, 5), thermal state with $v_t = 5$, and single-mode squeezed vacuum state with $r_s = 0.5$ and with $\hat{q}$ quadrature being squeezed.

The Gaussian entangled squeezed states can be generated by parametric down conversion in a non-degenerate optical parametric amplifier [119]–[123], where a crystal having an optical nonlinearity is pumped by a bright laser beam. A photon of the incoming pumping beam spontaneously transfigures in the non-linear crystal into a lower-energy pair of photons, termed as the signal and the idler [119]–[123]. In Type-II parametric down conversion, which is known as a source of entangled states in the CV domain, the signal and idler are in orthogonal polarizations, forming a Gaussian entangled squeezed state [119]–[123]. In this process, the pump photons of frequency $2\omega_p$ are converted into pairs of entangled photons having a pair of different-frequency modes, namely modes 1 and 2 of frequency ω_1 and ω_2, where $2\omega_p = \omega_1 + \omega_2$. An alternative way of generating the Gaussian entangled squeezed state is by mixing two orthogonally single-mode squeezed vacuum states, where one of the states is squeezed in the $\hat{q}$

quadrature and the other one is squeezed in the $\hat{p}$ quadrature. This mixing can be achieved by a balanced (or 50:50) beam splitter. Note that the single-mode squeezed vacuum state can be generated by Type-I parametric down conversion in a degenerate optical parametric amplifier, where the pump photons of frequency $2\omega_p$ are split into pairs of photons having the same frequency and polarization [123].

Finally, note that by invoking local unitary operators the first moment of every two-mode Gaussian state can be set to zero and the covariance matrix can be transformed into the following standard form [86], [87], [114]

$$\boldsymbol{M_s} = \begin{pmatrix} \boldsymbol{A} & \boldsymbol{C} \\ \boldsymbol{C}^T & \boldsymbol{B} \end{pmatrix}, \tag{20}$$

where we have $\boldsymbol{A} = a\boldsymbol{I}$, $\boldsymbol{B} = b\boldsymbol{I}$, $\boldsymbol{C} = diag(c_+, c_-)$, $a, b, c_+, c_- \in \mathbb{R}$.

B. Homodyne Detection

The homodyne detection of Fig. 9(a) represents the most common measurement in CV quantum information processing [9], [86], [87]. This detection scheme can be used for determining or observing the quadrature operator $\hat{q}$ (or $\hat{p}$) of a mode. The scheme of Fig. 9(a) is experimentally implemented by combining the target mode (relying on the annihilation operator $\hat{a}$) with a local oscillator via a balanced beam splitter. The local oscillator is assumed to be in a bright coherent state $|\alpha_{LO}\rangle$. Since $|\alpha_{LO}\rangle$ is represented by a large number of photons, the local oscillator can be described by a classical complex amplitude α_{LO}. The two output modes of the beam splitter can then be approximated by $\hat{a}_1 = (\alpha_{LO} + \hat{a})/\sqrt{2}$ and $\hat{a}_2 = (\alpha_{LO} - \hat{a})/\sqrt{2}$.

The intensity of each outgoing mode is then measured using a photodetector, which converts the photons of the electromagnetic mode into electrons, and hence into an electric current - which is termed as the photo-current $\hat{i}$. The photo-current is proportional to the number of photons in the electromagnetic mode. Hence, the pair of photodetectors of the two output modes of the beam splitter generate the photo-currents of

$$\begin{aligned} \hat{i}_1 \propto \hat{n}_1 = \hat{a}_1^\dagger \hat{a}_1 = \left(\alpha_{LO}^* + \hat{a}^\dagger\right)(\alpha_{LO} + \hat{a})/2, \\ \hat{i}_2 \propto \hat{n}_2 = \hat{a}_2^\dagger \hat{a}_2 = \left(\alpha_{LO}^* - \hat{a}^\dagger\right)(\alpha_{LO} - \hat{a})/2. \end{aligned} \tag{21}$$

Then the difference between the photo-currents $\hat{i}_1$ and $\hat{i}_2$ is measured, or more specifically, $\hat{i}_1 - \hat{i}_2 \propto (\alpha_{LO}^* \hat{a} + \alpha_{LO} \hat{a}^\dagger)$ is measured. Considering a local oscillator associated with $\alpha_{LO} = |\alpha_{LO}| \exp(i\Theta)$, where $|\alpha_{LO}|$ and Θ are the magnitude and phase of the local oscillator respectively, the quadrature operator $\hat{q}$ ($\hat{p}$) can be measured by setting the local oscillator's phase as $\Theta = 0$ ($\Theta = \pi/2$).

In contrast to homodyne detection, heterodyne detection allows us to measure both the quadrature operators $\hat{q}$ and $\hat{p}$ of a mode simultaneously [9], [86], [87]. A heterodyne detector combines the target mode with a vacuum ancillary mode into a balanced beam splitter. Then, homodyne detection is applied to the conjugate quadratures of the two output modes, i.e., to $\hat{q}$ of one output mode and $\hat{p}$ of the other one, which are measured using homodyne detection. The 'price' to pay for this simultaneous detection is the introduction of an additional noise term into the measurements (due to the mixing into the signal of the vacuum state). The implementation of heterodyne detection is shown in Fig. 9(b).

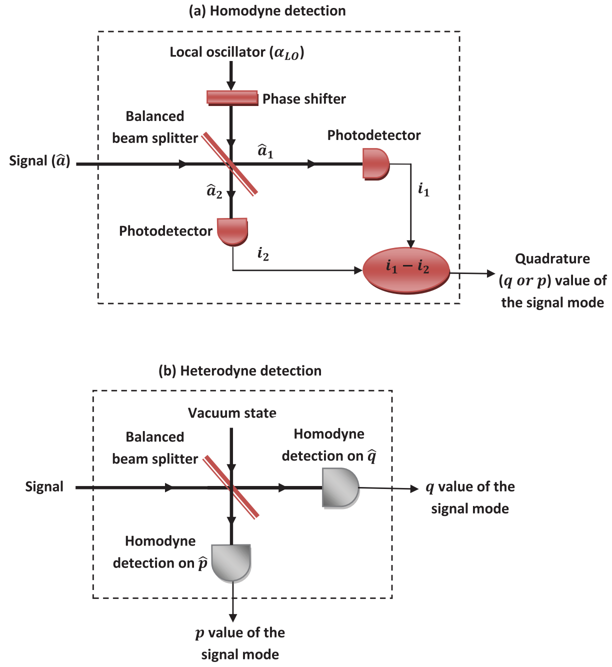


Fig. 9. (a) Homodyne detection: The signal mode is combined with the local oscillator in a balanced beam splitter. Each output mode of the beam splitter is then measured using a photodetector, which generates a photocurrent proportional to the photon numbers of the output mode. By measuring the difference between the two photo-currents, the $\hat{q}$ (or $\hat{p}$) quadrature operator of the signal mode can be measured depending on the phase of the local oscillator. (b) Heterodyne detection: The signal mode interacts with a vacuum mode in a balanced beam splitter. By applying homodyne detection to the conjugate quadratures of the two output modes, both the quadrature operators of the signal mode can be measured simultaneously at the price of introducing an additional noise term into the measurements.

C. CV Entanglement

We have already discussed the notion of entanglement. Indeed, this property is one of the most important properties of quantum mechanics, and is widely recognized as a basic resource for quantum information processing and quantum communications (for review, see [83], [87], [113], [114]). We now attempt to quantify the entanglement property of CV states more carefully. We focus our attention on *bipartite* CV entanglement, which relies on the entanglement between two CV quantum systems. Let us consider the pair of CV quantum systems A and B having Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. The Hilbert space of the composite system is given by the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$. By definition, a bipartite quantum state $\hat{\rho}_{AB}$ relying on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is said to be separable, if it can be formulated as a probability distribution over a pair of uncorrelated states expressed as $\hat{\rho}_{AB} = \sum_i p_i \hat{\rho}_i^A \otimes \hat{\rho}_i^B$, where the quantum state $\hat{\rho}_i^A$ ($\hat{\rho}_i^B$) acts on the Hilbert space $\mathcal{H}_A$ ($\mathcal{H}_B$), $p_i \geq 0$, and $\sum_i p_i = 1$. If a quantum state $\hat{\rho}_{AB}$ is separable, then its partial transpose $\hat{\rho}_{AB}^{PT}$ with respect to either subsystem is positive [124]. The partial transposition of $\hat{\rho}_{AB}$ represents the transposition with respect to only one of the two subsystems, for example to system *B*. By definition, a state is stated to be entangled, when it is not separable in the above-mentioned sense.

The *grade* (or quantifiable measure) of entanglement in a *pure* bipartite quantum state $|\psi\rangle$ (with density operator $\hat{\rho}_{AB} = |\psi\rangle\langle\psi|$) can be quantified by the entropy of entanglement $E_v(|\psi\rangle)$. The entropy of entanglement stipulates the number of entangled qubits (measured in ebits)[15] that can be extracted from the state. It also can be considered as the amount of entanglement required to generate the state. The entropy of entanglement is given by the von Neumann entropy of the reduced density operators $\hat{\rho}_A$ or $\hat{\rho}_B$, where $\hat{\rho}_A = \mathrm{Tr}_B(\hat{\rho}_{AB})$ and $\hat{\rho}_B = \mathrm{Tr}_A(\hat{\rho}_{AB})$, with Tr_A and Tr_B denoting the partial trace [83], [87], [113], [114].

For a Gaussian state $\hat{\rho}$, the von Neumann entropy $S(\hat{\rho})$ is given by $S(\hat{\rho}) = \sum_k g(\nu_k)$, where we have $g(x) = [(x+1)/2]\log_2[(x+1)/2] - [(x-1)/2]\log_2[(x-1)/2]$, and ν_k are the symplectic eigenvalues[16] of the covariance matrix of the state. For a pure two-mode entangled state in the form of $|\psi\rangle = \sum_{n=0}^{\infty} q_n |n\rangle_1 |n\rangle_2$, the entropy of entanglement is given by $E_v(|\psi\rangle) = -\sum_{n=0}^{\infty} q_n^2 \log_2 q_n^2$.

Among the different quantifiable measures used as a grade of entanglement for a *mixed* bipartite quantum state $\hat{\rho}_{AB} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, the most well-known is perhaps the entanglement of formation [125], [126], E_f. This is defined as $E_f(\hat{\rho}_{AB}) = \min\limits_{\{p_i, |\psi_i\rangle\}} \sum_i p_i E_v(|\psi_i\rangle)$, where the minimum is taken over all the possible pure-state decompositions of the mixed state $\hat{\rho}_{AB}$. The entanglement of formation gives the minimal amount of entanglement of any ensemble of pure states realizing the given state $\hat{\rho}_{AB}$ - meaning it quantifies the minimum amount of entanglement needed to prepare the quantum state $\hat{\rho}_{AB}$ from a mix of pure entangled states. In fact, given an entangled state $\hat{\rho}_{AB}$, the entanglement of formation expresses the number of maximally entangled states we need to create $\hat{\rho}_{AB}$. In general, this measure of entanglement is difficult to calculate.

The distillable entanglement is another measure for entanglement, and is the amount of entanglement that can be distilled from a given mixed state [113]. This quantity is also hard to calculate in general, since it would require optimization over all possible distillation protocols. However, there is an entanglement measure which is easy to compute, and gives an upper bound on the amount of distillable entanglement. This measure is the so-called logarithmic negativity [127], [128].

The logarithmic negativity (LN) exhibits the following properties. (i) E_{LN} is a non-negative function, $E_{LN}(\hat{\rho}_{AB}) \geq 0$. (ii) If $\hat{\rho}_{AB}$ is separable, $E_{LN}(\hat{\rho}_{AB}) = 0$. (iii) $E_{LN}(\hat{\rho}_{AB})$ does not increase on average under local (quantum) operations and classical communications. The logarithmic negativity of a bipartite state $\hat{\rho}_{AB}$ is defined as [127]

$$E_{LN}(\hat{\rho}_{AB}) = \log_2[1 + 2N(\hat{\rho}_{AB})], \tag{22}$$

where $N(\hat{\rho}_{AB})$ is the negativity defined as the absolute value of the sum of the negative eigenvalues of $\hat{\rho}_{AB}^{PT}$. The logarithmic negativity quantifies as to what degree the quantum state fails to satisfy the positivity of the partial transpose condition.

In the special case of two-mode Gaussian states, we are able to determine the logarithmic negativity through the use of the covariance matrix [83], [87], [114]. Given a two-mode Gaussian state associated with a covariance matrix $\boldsymbol{M} = \{\boldsymbol{A}, \boldsymbol{C}; \boldsymbol{C}^T, \boldsymbol{B}\}$ where $\boldsymbol{A} = \boldsymbol{A}^T$, $\boldsymbol{B} = \boldsymbol{B}^T$, and $\boldsymbol{C}$ are 2×2 real matrices, the logarithmic negativity is given by [83], [87], [114]

$$E_{LN}(\boldsymbol{M}) = \max[0, -\log_2(\tilde{\nu}_-)], \tag{23}$$

where $\tilde{\nu}_-$ is the smallest symplectic eigenvalue of the partially transposed $\boldsymbol{M}$. This eigenvalue is given by [83], [87], [114]

$$\tilde{\nu}_-^2 = \left(\Delta - \sqrt{\Delta^2 - 4\det(\boldsymbol{M})}\right)/2, \tag{24}$$

where $\Delta = \det(\boldsymbol{A}) + \det(\boldsymbol{B}) - 2\det(\boldsymbol{C})$.

D. Gaussian Lossy Quantum Channel

Consider a fixed-attenuation channel described by a transmissivity of $0 \leq \tau \leq 1$ and thermal noise variance of $V_n \geq 1$. Note that in the optical frequency domain the average number of photons is very low even at room temperature (300K), hence the thermal noise has a negligible impact on the signal. In fact, in the optical frequency domain the noise variance is effectively unity, simply representing the vacuum noise. However, in the millimeter-wave domain the thermal noise exhibits a variance, V_n, which is much higher than unity. More specifically, we have $V_n = 2\bar{n} + 1$ with $\bar{n}$ being the average number of photons [129]–[132]. In order to suppress the thermal noise, the system has to be operated at very low temperatures, e.g., <100mK. The average number of photons for a single mode is given by [129]–[132] $\bar{n} = [\exp(hf/k_B T_b) - 1]^{-1}$, where f is the frequency of the mode, k_B is the Boltzmann's constant, and T_b is the temperature.

A fixed-attenuation channel is a Gaussian channel, which transforms the Gaussian input states into Gaussian states. For example, if a single-mode Gaussian quantum state is transmitted through a fixed-attenuation channel, it will remain Gaussian at the output of the channel even though it has experienced channel loss. We can model the impact of a fixed-attenuation channel of transmissivity τ and thermal noise variance V_n on the single-mode input Gaussian state $\hat{\rho}$ by a beam splitter transformation, with the transmissivity of the beam splitter being τ and reflectivity $1-\tau$. In this channel representation shown in Fig. 10 the Gaussian input state is

[15] An ebit (entanglement qubit) as the unit of bipartite entanglement is the amount of entanglement that is contained in a maximally entangled two-qubit state (Bell state). In fact, it is said that each of the Bell states contains one ebit of entanglement.

[16] For an arbitrary N-mode covariance matrix $\boldsymbol{M}$, there exists a symplectic matrix $\boldsymbol{S}$ such that $\boldsymbol{M} = \boldsymbol{S}\boldsymbol{M_d}\boldsymbol{S}^T$, where $\boldsymbol{M_d} = \bigoplus_{k=1}^{N} \nu_k \boldsymbol{I}$ is a diagonal matrix, and the N positive quantities ν_k are the symplectic eigenvalues of $\boldsymbol{M}$. Note that a symplectic matrix $\boldsymbol{S}$ is a matrix with real elements that satisfies the condition $\boldsymbol{S}\boldsymbol{\Omega}\boldsymbol{S}^T = \boldsymbol{\Omega}$ where $\boldsymbol{\Omega}$ is defined in Eq. (14) [87], [114]. For example, given a two-mode Gaussian state associated with a covariance matrix $\boldsymbol{M} = \{\boldsymbol{A}, \boldsymbol{C}; \boldsymbol{C}^T, \boldsymbol{B}\}$, where $\boldsymbol{A} = \boldsymbol{A}^T$, $\boldsymbol{B} = \boldsymbol{B}^T$, and $\boldsymbol{C}$ are 2×2 real matrices, the symplectic eigenvalues of $\boldsymbol{M}$ are given by $\nu_\pm^2 = (\Delta \pm \sqrt{\Delta^2 - 4\det(\boldsymbol{M})})/2$, where $\Delta = \det(\boldsymbol{A}) + \det(\boldsymbol{B}) + 2\det(\boldsymbol{C})$ [87], [114].

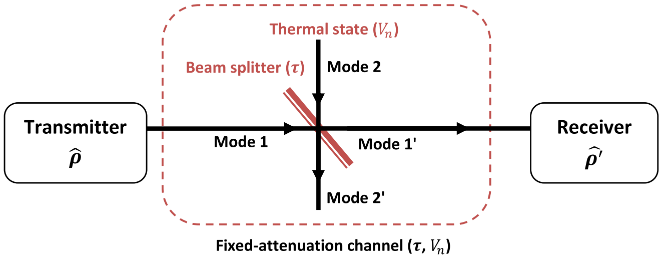


Fig. 10. The beam splitter representation of a fixed-attenuation channel with transmissivity τ and thermal noise variance V_n. In this channel representation, the transmitted signal mode is combined with a thermal mode of variance V_n in a beam splitter of transmissivity τ. In the case of a pure-attenuation channel (without thermal noise), the signal mode is simply combined with a vacuum mode of variance $V_n = 1$.

combined with the thermal noise in the beam splitter, such that one input mode of the beam splitter is the Gaussian input state $\hat{\rho}$ having the corresponding quadratures of $\hat{q}_1, \hat{p}_1$ and the second input mode is the thermal noise with corresponding quadratures of $\hat{q}_2, \hat{p}_2$. As a result of the beam splitter transformation we have the output modes $1'$ (corresponding to the received quantum state $\hat{\rho}'$ at the output of the channel) and $2'$ with corresponding quadratures of $\hat{q}_1', \hat{p}_1'$ and $\hat{q}_2', \hat{p}_2'$ respectively. These output quadratures can be described by [87]

$$\hat{R}_{out} = \begin{pmatrix} \sqrt{\tau}\boldsymbol{I} & \sqrt{1-\tau}\boldsymbol{I} \\ -\sqrt{1-\tau}\boldsymbol{I} & \sqrt{\tau}\boldsymbol{I} \end{pmatrix} \hat{R}_{in}, \tag{25}$$

where $\hat{R}_{in} = (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2)$, and $\hat{R}_{out} = (\hat{q}_1', \hat{p}_1', \hat{q}_2', \hat{p}_2')$. As a result, the quadrature variance of the received quantum state at the output of the channel is given by $V(\hat{q}_1') = \tau V(\hat{q}_1) + (1-\tau) V_n$, and $V(\hat{p}_1') = \tau V(\hat{p}_1) + (1-\tau) V_n$.

Let us now use such a channel representation to analyse the evolution of a two-mode Gaussian quantum state over a fixed-attenuation channel (the general multimode case can be significantly more complex, e.g., [133]). We consider a TMSV state with zero mean and covariance matrix in the form of Eq. (19) as the input quantum state of the channel. There are two settings for the transmission of a two-mode quantum state between two parties, namely, the single-mode transfer and the two-mode transfer [134]. We discuss each of these in detail.

Single-mode transfer: In this setting, the TMSV source is placed at one of the parties' site. In this case, only one mode (mode 2) is transmitted through a fixed-attenuation channel, with the other mode (mode 1) remaining unaffected. The Gaussian output state has a zero mean and covariance matrix in the following form [87], [134]

$$\boldsymbol{M_{sm}} = \begin{pmatrix} v\boldsymbol{I} & \sqrt{\tau}\sqrt{v^2-1}\boldsymbol{Z} \\ \sqrt{\tau}\sqrt{v^2-1}\boldsymbol{Z} & (\tau v + (1-\tau) V_n)\boldsymbol{I} \end{pmatrix}, \tag{26}$$

where $v = \cosh\,(2r)$ is the quadrature variance of each mode in the input TMSV state (r being the two-mode squeezing parameter).

Two-mode transfer: In this setting, the TMSV source is placed somewhere between the two parties. In this case, one mode (mode 1) of the TMSV state is transmitted through a fixed-attenuation channel with transmissivity τ_1 and thermal noise variance V_{n1}, while the other mode (mode 2) being transmitted through another fixed-attenuation channel with transmissivity τ_2 and thermal noise variance V_{n2}. The Gaussian output state has a zero mean and covariance matrix in the following form [87], [134]

$$\boldsymbol{M_{tm}} = \begin{pmatrix} (\tau_1 v + (1-\tau_1) V_{n1})\boldsymbol{I} & \sqrt{\tau_1\tau_2}\sqrt{v^2-1}\boldsymbol{Z} \\ \sqrt{\tau_1\tau_2}\sqrt{v^2-1}\boldsymbol{Z} & (\tau_2 v + (1-\tau_2) V_{n2})\boldsymbol{I} \end{pmatrix}. \tag{27}$$

Here, we have assumed that the pair of fixed-attenuation channels are independent and that the two thermal noises are uncorrelated.

IV. Continuous Variable Quantum Key Distribution

CV-QKD protocols using Gaussian quantum states have been richly analysed in theory [12], [13], [15], [87], [118], [135], [136], and they have also been implemented experimentally [14], [20], [21], [23]–[25], [80], [137]–[140]. Among these contributions, the authors of [12]–[14], [20], [21], [23]–[25], [118], and [137]–[140] exploit the so-called prepare-and-measure (PM) scheme, where Alice prepares CV quantum states and encodes the key information onto the quantum states, which are then transmitted over an insecure quantum channel to Bob. At the output of the channel Bob receives the quantum states and measures them using classical homodyne or heterodyne detectors. As a result, correlated, but non-identical, data is created between Alice and Bob. Each PM scheme of CV-QKD can be represented by an equivalent entanglement-based (EB) scheme [15], [80], [87], [118], [135], [136], where Alice generates a two-mode entangled state,[17] with one mode being held by Alice and the other mode being transmitted through an insecure quantum channel to Bob. Again, Alice and Bob then proceed by measuring/observing their own modes using classical homodyne or heterodyne detectors in order to create correlated but non-identical data. Following the generation of the correlated data, Alice and Bob proceed with classical post-processing over a public, but authenticated, classical channel (in both the PM scheme and EB scheme), so as to generate a key, which remains secret even in the presence of Eve.

A. Prepare-and-Measure Approach

The PM CV-QKD is derived from the classic DV BB84 protocol of [3]. Hence, for the sake of enhancing readability, we commence by detailing the DV BB84 protocol before delving deeper into the specific instantiations of PM CV-QKD.

The DV BB84 protocol, conceived in 1984, is named after its inventors Bennett and Brassard. It derives it's strength from the two fundamental laws of quantum physics, namely the 'no-cloning theorem' and the 'measurement' of Fig. 3. Table III lists an example of the DV BB84 protocol, which proceeds as follows:

1) Alice generates a string of random bits, called the 'raw key', which is much longer than the desired length of the key.

[17] Please refer to Section III-C for CV entanglement.

TABLE III

Prepare-and-Measure Discrete Variable BB84 QKD Example (in the Absence of Eve and Noise). (1) Random Binary Key Generated. (2) Rectilinear or Diagonal Polarization Randomly Selected. (3) Quantum State Prepared by Encoding the Binary Key of Step (1) Using the Polarizations of Step (2). (4) Measurement Basis Randomly Selected. Instances Where the Preparation and Measurement Basis Match Are Marked in Green. (5) Received States Measured Using the Basis of Step (4). (6) Detected States Mapped Onto Bits. Instances Where the Detected and Raw Key Bits Differ Are Marked in Red. (7) Only Those Bits Retained, Which Have the Same Preparation and Measurement Basis. (8) Error Rate Estimated for Detecting the Presence of Eve. (9) Information Reconciliation Corrects Errors in the Sifted Key. (10) Corrected Key Further Shortened Using Privacy Amplification, Hence Reducing Eve's Information About the Key

Alice													
1	Raw key	1	0	0	1	1	1	0	1	0	0	0	1
2	Preparation (or encoding) basis	+	+	×	×	+	×	+	+	×	×	+	×
3	Quantum state preparation	→	↑	↗	↘	→	↘	↑	→	↗	↗	↑	↘
Bob													
4	Measurement basis	+	×	×	+	×	×	+	×	×	+	+	+
5	Quantum state detected	→	↘	↗	→	↗	↘	↑	↘	↗	→	↑	→
6	Detected key	1	1	0	1	0	1	0	1	0	1	0	1
Classical post-processing													
7	Sifted key	1		0			1	0		0		0	
8	Parameter (or error) estimation												
9	Information reconciliation												
10	Privacy amplification												

2) Alice exploits two conjugate pairs of states for encoding the classical raw key into photon polarizations (qubits). Specifically, the states within the pair are orthogonal, while the two pairs are the conjugates of each other. In our example, we consider the rectilinear polarization ($+$ in Table III), which maps bit 0 and 1 onto the vertical ($\uparrow$) and horizontal ($\rightarrow$) polarizations, respectively, and the diagonal polarization ($\times$ in Table III), which maps bit 0 and 1 onto the 45° ($\nearrow$) and 135° ($\searrow$) polarizations, respectively. Alice randomly chooses either the rectilinear or diagonal polarization for the action termed as state preparation.
3) Alice encodes the raw key of Step (1) seen in Table III based on the randomly chosen polarizations of Step (2) in Table III using $+$ or $\times$ and sends the resultant qubits to Bob over an insecure quantum channel.
4) Neither Bob nor Eve knows the encoding basis of Step (2) in Table III used by Alice. Therefore, Bob randomly chooses either the rectilinear ($+$) or the diagonal ($\times$) basis for measuring the received qubits. Bob's chosen basis are listed in Step (4) of Table III. Since both Alice and Bob randomly choose the polarization basis, they will end up choosing the same basis roughly half of the time. These instances have been marked in green in Steps (2) and (4) of Table III.
5) If Bob measures the qubits received in the same basis as they were prepared in Step (2) of Table III, then he detects the transmitted bit correctly, provided that the quantum channel is noiseless and there is no eavesdropper. By contrast, if the measurement basis is not the same as the preparation basis, then there is only a 50% chance that Bob will detect the bit correctly. For example, let us consider the second bit of Table III having the value 0, which is encoded in the rectilinear basis ($+$), but measured in the diagonal basis ($\times$). A bit value 0 in the rectilinear basis may also be expressed as a function of the diagonal basis:
$$|\uparrow\rangle \equiv \frac{1}{\sqrt{2}}|\nearrow\rangle + \frac{1}{\sqrt{2}}|\searrow\rangle. \tag{28}$$
Consequently, when $\uparrow$ is measured in the diagonal basis, it is equally likely to collapse either to the state $|\nearrow\rangle$ (bit 0) or the state $|\searrow\rangle$ (bit 1).
6) The detected polarizations of Step (5) may be decoded by invoking the same classical-to-quantum mapping as the encoding operation at the transmitter. Bob detects the bit correctly approximately 75% of the time. All incorrect instances of bit detection are marked in red in Steps (1) and (6) of Table III. Hence, Alice and Bob acquire a correlated key through Steps (1) to (6).
7) Alice and Bob then communicate over an authenticated classical channel for further processing the correlated key they possess, hence termed as 'classical post-processing'. This post-processing commences with 'bit sifting' during which Alice shares the basis used for preparation in Step (2) of Table III, while Bob shares the basis of Step (5) in Table III used for measurement. Both Alice and Bob discard the specific bits whose preparation basis and measurement basis differ, because these instances may result in incorrect detection, which are marked in red in Step (6) of Table III and statistically represent about 25% of the bits. This in turn ensures that both Alice and Bob possess the same secret key in the absence of Eve, provided that the quantum channel is noiseless. The length of this key is approximately half of that of the raw key, in which about half of the basis were different.
8) Recall that qubits cannot be cloned. Therefore, if Eve is listening to the insecure quantum channel, she cannot acquire a copy of the quantum information. Furthermore, Eve unaware of the specific basis in which Alice maps the classical bits onto the qubits, until Alice reveals this information during the classical post-processing stage. Consequently, similar to Bob, Eve chooses a random basis for measurement, while listening to the quantum-domain session between Alice and Bob. This in turn introduces errors in the shared key. Hence, for the sake of determining the presence of Eve, Alice and Bob share a subset of the key and

estimate the fraction of errors. If the resultant error ratio is higher than a pre-determined threshold, the transmission is considered 'insecure' and hence aborted.

9) By contrast, if the transmission is found to be secure, the process termed as 'information reconciliation' is invoked for correcting the dependencies between Alice's and Bob's key, which may include for example the dependencies arising from errors inflicted by a realistic imperfect quantum channel as well as those due to measurements by Eve. Let us now briefly elaborate on the effect of channel errors. Consider the first bit of Table III, which is prepared and measured in the same basis. As shown in Table III, Alice transmits the quantum state $|\rightarrow\rangle$ corresponding to the classical bit 1. Let us consider the scenario where a channel error is inflicted on Alice's quantum state during transmission, so that Bob receives the erroneous state $|\uparrow\rangle$. Now even if Bob measures the received quantum state in the same basis as it was prepared, his detected output will be incorrect. Explicitly, Bob will detect bit 0 upon measurement in the rectilinear basis $(+)$, while Alice transmitted bit 1. Hence, channel errors also introduce dependencies between Alice's and Bob's keys.

10) Eve may acquire information about the secret key by measuring a subset of the key as well as by listening to the public classical information shared during the error reconciliation process. For the sake of reducing this information, the technique of 'privacy amplification' is invoked. Explicitly, privacy amplification generates a shorter key from the corrected key of Step (9), hence reducing Eve's information about the shared key.

In contrast to the PM DV-QKD scheme of Table III, which transmits qubits, a Gaussian PM CV-QKD scheme exploits Gaussian CV quantum states, as shown in Fig. 11.

Explicitly, the CV quantum states prepared by Alice are Gaussian states (squeezed states or coherent states) which are modulated by Gaussian distributions [12]–[14], [20], [21], [24], [25], [118], [135], [137], [138], [140]. In fact, Alice encodes a classical random variable drawn from a Gaussian distribution onto a Gaussian quantum state, which is transmitted to Bob, and then measured by him, thus extracting a classical random variable which is correlated with Alice's. Furthermore, in contrast to the discrete measurement operations of Table III, the measurements of the received quantum states are made by Gaussian measurements, namely by classical homodyne or heterodyne detection. Hence, Alice and Bob share correlated Gaussian data in contrast to the correlated binary stream of PM DV-QKD. The resultant correlated Gaussian distributed random variable (rv) is then processed classically for the sake of generating a virtually error free and secure binary key.

We may notice in Fig. 11 that four different variants of a Gaussian PM CV-QKD protocol exist, since we have two types of Gaussian quantum states, i.e., squeezed and coherent states, and two types of detectors, i.e., homodyne and heterodyne detectors, which are detailed in Section III. In the succeeding subsections, we provide further insights into each of these four variants with the aid of slow-paced quantitative examples.

1) PM CV-QKD Relying on Squeezed States & Homodyne Detection: Table IV gives an example of CV-QKD protocol using squeezed states and homodyne detection [12], which proceeds as follows:

1) Alice generates a real random Gaussian-distributed variable a with zero mean $\mu = 0$ and variance $\sigma^2 = v_m$, as exemplified in Step (1) of Table IV.

2) Alice then decides to encode the Gaussian variable a into either a *p*-squeezed or a *q*-squeezed vacuum state by randomly choosing the $\hat{p}$ or $\hat{q}$ quadrature component for squeezing. More specifically, Alice generates a binary random variable *u* for choosing the $\hat{p}$ or $\hat{q}$ quadrature for squeezing. The chosen quadratures are listed in Step (2) of Table IV.

3) Alice next proceeds with quantum state preparation. Explicitly, Alice prepares a single-mode squeezed vacuum state having the covariance matrix $\boldsymbol{M} = diag(1/v, v)$, where $v = \exp(2r_s)$, and r_s is the single-mode squeezing. The prepared squeezed state is then modulated (displaced) by an amount a of Step (1) in Table IV, where the modulation variance satisfies $v_m = v - 1/v$. Specifically, depending on the quadratures chosen in Step (2) of Table IV, Alice either sends a *q*-squeezed state having a first moment of $(a_q, 0)$, $a_q = a$, or a *p*-squeezed state associated with the first moment $(0,\ a_p)$, $a_p = a$, as illustrated in Step (3) of Table IV. For example, let us consider the first element of raw Gaussian key having the value of 0.9 in Step (1) of Table IV. Since $\hat{p}$ quadrature is chosen in Step (2) of Table IV for preparing the first quantum state, Alice prepares a *p*-squeezed state having the first moment (0, 0.9). The prepared and modulated squeezed states are then transmitted over an insecure quantum channel to Bob.

4) For each incoming quantum state, Bob randomly chooses either the $\hat{q}$ or the $\hat{p}$ quadrature for detection depending on his own binary random variable u', as shown in Step (4) of Table IV.

5) Bob measures the received quantum state in either the $\hat{q}$ or the $\hat{p}$ quadrature using homodyne detection based on the chosen quadratures of Step (4). Note that in order to warrant security, Alice and Bob choose different basis for preparation and measurement (in a random fashion). Consequently, when the preparation and measurement basis are the same, which are marked in green in Steps (2) and (4) of Table IV, Bob accurately detects the transmitted quantum state, provided that the transmission channel is noiseless and there is no eavesdropper. For example, Bob chooses $\hat{p}$ quadrature for the first element of Gaussian key, as shown in Step (4) of Table IV. Since the first element was also prepared in the same quadrature, Bob correctly detects a $\hat{p}$-squeezed state having the first moment (0,0.9). By contrast, if the preparation and detection quadratures do not match, Bob detects a modified version of the transmitted state, which are marked as blank red cells in Table IV.

6) Finally, Bob obtains a real variable $b_q = b$ or $b_p = b$ corresponding to the $\hat{q}$ or the $\hat{p}$ detection quadratures.

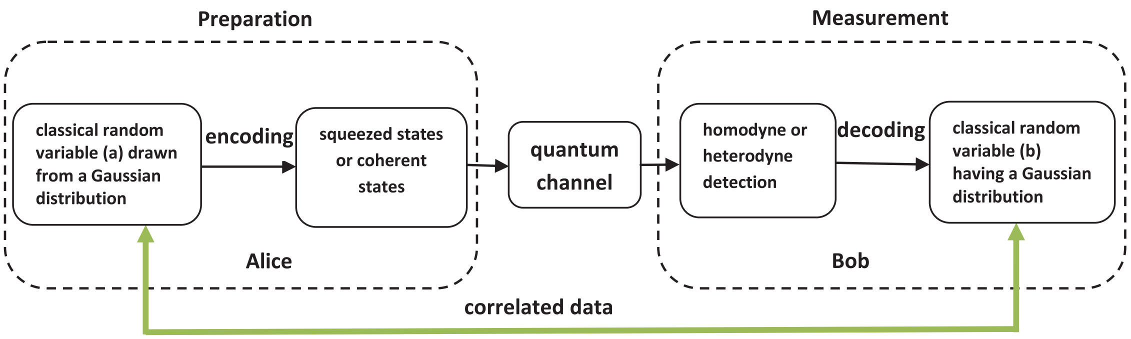

Preparation
Measurement
classical random variable (a) drawn from a Gaussian distribution
encoding
squeezed states or coherent states
quantum channel
homodyne or heterodyne detection
decoding
classical random variable (b) having a Gaussian distribution
Alice
Bob
correlated data

Fig. 11. The quantum communication stage of Gaussian CV-QKD protocol in a PM scheme, which consists of three steps; preparation, transmission, and detection. In a full-Gaussian protocol Alice encodes a classical Gaussian-distributed random variable (*a*) onto Gaussian quantum states (squeezed or coherent states). The prepared states are transmitted through an insecure quantum channel to Bob. In the detection step, received quantum states are measured using Gaussian measurements (homodyne or heterodyne detection) to obtain a classical Gaussian-distributed random variable (*b*), which is correlated with Alice's random variable (*a*).

TABLE IV

Prepare-and-Measure CV-QKD Example Relying on Squeezed States and Homodyne Detection (in the Absence of Eve and Noise). (1) Real Random Variable *a* Generated Using a Gaussian Distribution Having Mean $\mu = 0$ and Variance $\sigma^2 = v_m$. (2) $\hat{p}$ or $\hat{q}$ Quadrature Randomly Chosen for Squeezing. (3) Squeezed State Prepared Having the First Moment (a, 0), if $\hat{q}$ Quadrature Is Chosen in Step (2) and the Moment (0, a), If $\hat{p}$ Quadrature Is Chosen in Step (2). (4) $\hat{p}$ or $\hat{q}$ Detection Quadrature Randomly Selected. Instances Where the Preparation and Detection Quadratures Match Are Marked in Green. (5) Received States Detected Using the Quadratures of Step (4). The Detection Outcome Is Noisy (or Corrupted), When the Preparation and Detection Basis Do Not Match, Hence Are Marked in Red. (6) Detected States Mapped Onto Gaussian Key. (7) Only Those Key Values Are Retained, Which Have the Same Preparation and Measurement Quadrature

Alice													
1	Raw Gaussian key ($\mu = 0$, $\sigma^2 = v_m$)	0.9	2.4	1.3	2.1	0.5	4.1	1.1	0.3	3.6	0.2	1.7	2.8
2	Preparation (or encoding) quadrature	$\hat{p}$	$\hat{p}$	$\hat{q}$	$\hat{q}$	$\hat{p}$	$\hat{q}$	$\hat{p}$	$\hat{p}$	$\hat{q}$	$\hat{q}$	$\hat{p}$	$\hat{q}$
3	Squeezed state preparation (first moment)	$(0, 0.9)$	$(0, 2.4)$	$(1.3, 0)$	$(2.1, 0)$	$(0, 0.5)$	$(4.1, 0)$	$(0, 1.1)$	$(0, 0.3)$	$(3.6, 0)$	$(0.2, 0)$	$(0, 1.7)$	$(2.8, 0)$
Bob													
4	Detection quadrature	$\hat{p}$	$\hat{q}$	$\hat{q}$	$\hat{p}$	$\hat{q}$	$\hat{q}$	$\hat{p}$	$\hat{q}$	$\hat{q}$	$\hat{p}$	$\hat{p}$	$\hat{p}$
5	Squeezed state detected (first moment)	$(0, 0.9)$	🟥	$(1.3, 0)$	🟥	🟥	$(4.1, 0)$	$(0, 1.1)$	🟥	$(3.6, 0)$	🟥	$(0, 1.7)$	🟥
6	Detected Gaussian key	0.9		1.3			4.1	1.1		3.6		1.7	
Classical post-processing													
7	Sifted Gaussian key	0.9		1.3			4.1	1.1		3.6		1.7	

The resulting variables constitute the detected Gaussian key, as shown in Step (6) of Table IV.

7) Following the measurement of all incoming states by Bob, classical post-processing over the public channel commences via a sifting operation. In this operation, Alice and Bob reveal to each other which of the two randomly selected quadratures they used for preparing (Alice) and measuring (Bob) the information, discarding non-tallying random bit pairs (i.e., $u \neq u'$). A natural way of achieving this is that Alice reveals for each Gaussian rv the specific value of u (i.e., whether she displaced the $\hat{q}$ or the $\hat{p}$ quadrature), and Bob only retains those, where he measured the relevant tallying quadrature (i.e., $u = u'$), as shown in Step (7) of Table IV.

Let us now consider the second variant of Fig. 11.

2) PM CV-QKD Relying on Squeezed States & Heterodyne Detection: Another squeezed-state protocol was developed in [118], in which Bob uses heterodyne detection rather than homodyne detection and measures both the $\hat{q}$ and $\hat{p}$ quadratures for obtaining (b_q, b_p). In the sifting step of this protocol, Bob then disregards one of his quadrature measurements, depending on Alice's specific choice of quadrature preparation. This protocol can be seen as a noisy version of the protocol with squeezed states and homodyne detection, since the heterodyne detection imposes vacuum noise on the measurement. When Bob's Gaussian rv are the reference of error correction (see below) in the classical post-processing, the heterodyne detection protocol exhibits a better robustness against the channel noise than the protocol associated with homodyne detection [118]. Let us now focus our attention on the third variant of Fig. 11.

3) PM CV-QKD Relying on Coherent States & Homodyne Detection: Table V gives an example of the PM CV-QKD protocol using coherent states and homodyne detection [13], [14], [116], which can be described as follows:

1) Alice generates random real numbers a_q chosen from an independent Gaussian distribution of variance v'_m.

TABLE V

PREPARE-AND-MEASURE CV-QKD EXAMPLE RELYING ON COHERENT STATES AND HOMODYNE DETECTION (IN THE ABSENCE OF EVE AND NOISE). (1) REAL RANDOM GAUSSIAN VARIABLE a_q GENERATED. (2) REAL RANDOM GAUSSIAN VARIABLE a_p GENERATED. (3) COHERENT STATE PREPARED HAVING A MEAN VALUE OF (a_q, a_p). (4) $\hat{p}$ OR $\hat{q}$ DETECTION QUADRATURE RANDOMLY SELECTED. (5) RECEIVED STATES DETECTED USING THE QUADRATURES OF STEP (4). (5) DETECTED STATES MAPPED ONTO GAUSSIAN KEY. (6) ALICE RETAINS a_q OR a_p DEPENDING ON BOB'S DETECTION QUADRATURES. THE RETAINED KEY VALUES ARE MARKED IN GREEN IN STEPS (1) AND (2)

Alice											
1	Raw Gaussian key (a_q)	0.9	2.4	1.3	2.1	0.5	4.1	1.1	0.3	3.6	0.2
2	Raw Gaussian key (a_p)	1.2	0.9	5.1	2.7	1.5	3.1	0.6	4.3	2.8	0.1
3	Coherent state preparation (mean)	$(0.9, 1.2)$	$(2.4, 0.9)$	$(1.3, 5.1)$	$(2.1, 2.7)$	$(0.5, 1.5)$	$(4.1, 3.1)$	$(1.1, 0.6)$	$(0.3, 4.3)$	$(3.6, 2.8)$	$(0.2, 0.1)$
Bob											
4	Detection quadrature	$\hat{p}$	$\hat{p}$	$\hat{q}$	$\hat{p}$	$\hat{q}$	$\hat{q}$	$\hat{p}$	$\hat{q}$	$\hat{q}$	$\hat{p}$
5	Detected Gaussian key	1.2	0.9	1.3	2.7	0.5	4.1	0.6	0.3	3.6	0.1
Classical post-processing											
6	Sifted Gaussian key	1.2	0.9	1.3	2.7	0.5	4.1	0.6	0.3	3.6	0.1

2) Alice also generates another set of random real numbers a_p, which are also chosen from an independent Gaussian distribution of variance v'_m.

3) Alice then prepares a coherent state, which is modulated (displaced) by the amounts of a_q and a_p generated previously in Steps (1) and (2), so that the resulting coherent state has a mean value of (a_q, a_p). For example, $a_q = 0.9$ and $a_p = 1.2$ are chosen for the first element of key in Steps (1) and (2), respectively. Consequently, Alice prepares a coherent state having a mean value of (0.9,1.2). The prepared coherent states transmitted over an insecure quantum channel to Bob.

4) Bob generates a random variable u' for each incoming state and chooses either the $\hat{q}$ or the $\hat{p}$ quadrature for detection depending on the value of u'.

5) Finally, Bob measures either the $\hat{q}$ or the $\hat{p}$ quadrature component using homodyne detection depending on the chosen quadratures of Step (4), hence obtaining a real variable b_q or b_p, respectively. For example, as can be seen in Table V, $\hat{p}$ quadrature is chosen in Step (4) for detecting the first element of the key. Consequently, when Bob measures the first received coherent state using the $\hat{p}$ quadrature, he obtains a value of 1.2.

6) When the quantum communication phase is completed and all the incoming states have been measured by Bob, classical post-processing over a public channel is commenced by applying sifting, where Bob reveals for each Gaussian rv the specific value of u' (i.e., whether he measured the $\hat{q}$ or the $\hat{p}$ quadrature), and Alice retains a_q or a_p depending on the value of u'. Note that in this protocol only one of the two real random variables generated by Alice is used for the key after the sifting stage. For example, Alice only retains $a_p = 1.2$ for the first element of key, since Bob measured the received state in the $\hat{p}$ quadrature. The retained key values are marked in green in Steps (1) and (2) of Table V.

Finally, we now consider the fourth variant of Fig. 11.

4) PM CV-QKD Relying on Coherent States & Heterodyne Detection: Another coherent-state protocol was developed in [117], where Bob uses heterodyne detection rather than homodyne detection and measures both the $\hat{q}$ and $\hat{p}$ quadrature components for obtaining (b_q, b_p) at the cost of imposing vacuum noise on the measurement. In this protocol, sifting is no longer needed, since both of the real random variables generated by Alice are used for the generation of the key, hence potentially resulting in higher secret key rates.

All the four CV-QKD protocols discussed above in the context of Fig. 11 yield a correlated Gaussian key between Alice and Bob. Please note that the Gaussian key generated in the examples above is the same for both Alice and Bob. However, when Eve is present or in the inevitable presence of noise, Bob's key will be a noisy version of Alice's key. Hence, Bob and Alice will possess correlated but unidentical Gaussian keys. Analogous to the PM DV-QKD of Table III, parameter estimation is then performed (in the classical post-processing stage, following the sifting step), where the two parties reveal a randomly chosen subset of their correlated but unidentical Gaussian key. This allows them to estimate the parameters of the channel, such as the channel's transmissivity and the level of channel noise, as well as to limit the maximum amount of information Eve can infer about their values. This step is followed by an information reconciliation procedure, which involves quantizing Alice's and Bob's correlated Gaussian data into binary keys as well as performing error correction, hence resulting in a near-error-free binary key. As discussed further later, this procedure normally relies on the employment of low density parity check (LDPC) codes [20]. QKD can be operated in two reconciliation scenarios, namely direct reconciliation [141] and reverse reconciliation [13], [14]. In the direct reconciliation protocol Alice's Gaussian data constitute the reference and she sends classical correction information to Bob which may be overheard by Eve. Then Bob corrects his key elements to arrive at the same values as Alice. By contrast, in the reverse reconciliation protocol Bob's Gaussian data constitute the reference and must be estimated by Alice (also by Eve) [13], [14]. Based on the upper bound on Eve's information estimated during the parameter estimation stage, Alice and Bob apply a privacy amplification protocol, which produces a shorter binary key in the spirit of expurgating Eve's information about the shared key, hence Eve's information about the key is substantially reduced.

Whilst in Fig. 11 we had four variants, now there are eight protocol choices for characterising Gaussian CV-QKD in a PM scheme. Explicitly, this is because we must consider

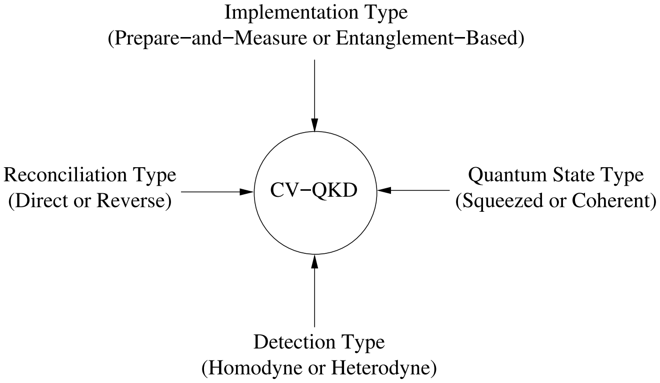


Fig. 12. Gaussian CV-QKD implementation parameters.

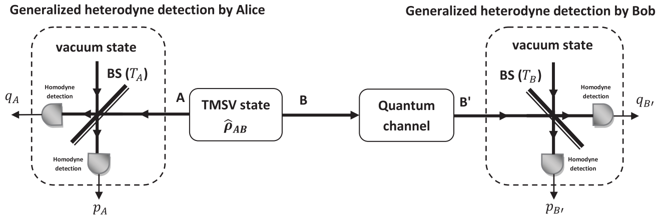


Fig. 13. The quantum communication stage of Gaussian CV-QKD protocol in an EB scheme. Alice generates a Gaussian two-mode entangled state (TMSV state) $\hat{\rho}_{AB}$. She keeps mode *A*, and sends mode *B* through an insecure quantum channel to Bob. If Alice applies homodyne detection, i.e., $T_A = 1$ (heterodyne detection, i.e., $T_A = 1/2$) to mode *A*, she remotely projects the other mode of the entangled state onto a squeezed state (coherent state). Similar to the PM scheme, Bob measures the received state using a Gaussian measurement (homodyne detection, i.e., $T_B = 1$ or heterodyne detection, i.e., $T_B = 1/2$). As a result of their measurements, Alice and Bob end up with two sets of classical Gaussian-distributed random variables which are correlated to each other.

both the type of quantum state (squeezed states or coherent states) which Alice prepares, and also the type of detection (homodyne or heterodyne detection) which Bob applies to the received states, as well as the specific type of reconciliation (direct reconciliation or reverse reconciliation). However, recall that all PM schemes have an equivalent EB scheme. Hence, different variants of CV-QKD may be implemented using the parameters summarized in Fig. 12. Next we discuss the entanglement-based approach for implementing CV-QKD protocols.

B. Entanglement-Based Approach

All the Gaussian PM protocols can be described in an unified way using the EB scheme [87], [135] shown in Fig. 13. Here Alice generates a TMSV state, which we refer to as $\hat{\rho}_{AB}$. She keeps mode *A*, and sends mode *B* to Bob. At some time later, Alice and Bob use an unbalanced beam splitter of transmissivity (T_A at Alice's side and T_B at Bob's side), to carry out *generalized heterodyne* detections. If Alice applies homodyne detection ($T_A = 1$), the prepared state should be a squeezed state and if Alice makes a heterodyne detection ($T_A = 1/2$), the prepared state should be a coherent state. The security of the CV-QKD protocols is mostly analysed using their equivalent EB scheme, where a two-mode entangled state is shared between Alice and Bob before their detection observations. Note, in the security analysis of CV-QKD discussed next we will assume that the number of exchanges between Alice and Bob is considered to be infinite (the asymptotic regime). This assumption is adopted in most QKD security analyses since the ability to estimate some quantities (e.g., average values) exactly in the infinite sample-limit, greatly simplifies the analyses.

C. CV-QKD Security Analysis

The most powerful, and most general, attack that Eve can implement against QKD is known as a coherent attack [87], [135]. In this attack, Eve prepares her ancillary system in a global quantum state, which means she prepares an arbitrary joint (entangled) state of the ancillae. After the interaction of the global ancillary system with the signals sent by Alice, the output ancillary system is stored in a quantum memory. Once the classical post-processing relying on the public channel is finished, Eve applies an optimal joint measurement over the ancillary system stored in the quantum memory to maximize her knowledge on the quantum information of the trusted parties. The security analysis of CV-QKD in the face of coherent attacks is very complex. However, under some trivial constraint imposed on the classical post-processing protocol, collective attacks are just as detrimental as coherent attacks [142]. In a collective attack against QKD Eve prepares her ancillary system in a product state of identically prepared ancillae. After interaction of each ancilla with a single signal sent by Alice, the output ancilla is stored in a quantum memory. Once the classical post-processing is completed, Eve applies an optimal joint measurement over the ensemble of ancillae in the quantum memory.

For a realistic reconciliation algorithm, the asymptotic CV-QKD key rate (bits per pulse) against collective attacks is given by [87] and [135] $K = \xi I_{AB} - I_E$, where I_{AB} is the mutual information between Alice and Bob (i.e., between Alice's variable, *a*, as well as Bob's variable, *b*), and 0< ξ <1 is the reconciliation efficiency. This efficiency reflects that in a realistic reconciliation algorithm, Alice and Bob acquire not all of the maximum attainable mutual information. Note that for a perfect reconciliation algorithm we will have $\xi = 1$. Furthermore, I_E is the Holevo bound defined in [87] and [135] as an upper bound on the quantum information stolen by Eve. In the reconciliation step, if we assume that Alice's data represents the reference, then $I_E = I_{AE}$ is the Holevo bound on the mutual information between Eve's quantum memory and Alice's variable. By contrast, if we assume that Bob's data is the reference, then $I_E = I_{BE}$ is the Holevo bound on the mutual information between Eve's quantum memory and Bob's variable. Note that I_{AB} remains the same, regardless of whose data represents the reference of reconciliation. It was also shown [143] that in the family of collective attacks, Gaussian attacks based on Gaussian operations[18] are

[18] Gaussian operations are linear operations with respect to the quadrature amplitudes. Such operations maintain the Gaussian character of Gaussian states.

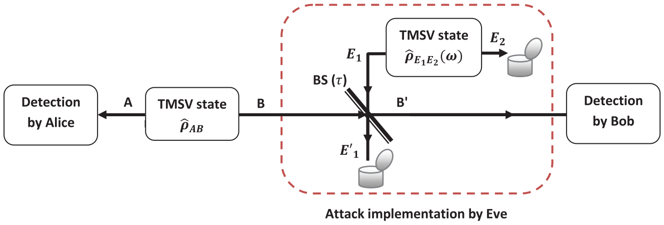

Detection by Alice
A
TMSV state $\hat{\rho}_{AB}$
B
BS (τ)
E_1
TMSV state $\hat{\rho}_{E_1E_2}(\omega)$
E_2
B'
Detection by Bob
E'_1
Attack implementation by Eve

Fig. 14. Implementation of optimal collective Gaussian attack (entangling-cloner attack) by Eve, in which Eve prepares an entangled state, $\hat{\rho}_{E_1E_2}$, interacts mode E_1 with the signal sent from Alice in a beam splitter (with the same transmissivity as the channel transmissivity). The output mode, mode B', is transmitted to Bob through a perfect quantum channel. The other output, mode E'_1, and the other arm of Eve's entangled state, mode E_2, are stored in Eve's quantum memory, to be collectively measured at the end of the classical post-processing.

the optimal attacks Eve can implement so as to minimize the secret key rate K.[19]

Let us consider a Gaussian CV-QKD protocol in the EB scheme, where Alice generates a TMSV state $\hat{\rho}_{AB}$, and keeps mode A while sending mode B to Bob over an insecure quantum channel. In the optimal collective Gaussian attack (which is also referred to as the entangling-cloner attack [14]) shown in Fig. 14, Eve models the quantum channel (with transmissivity of $0 \leq \tau \leq 1$ and thermal noise variance of $\omega \geq 1$) by a TMSV state $\hat{\rho}_{E_1E_2}$ having a quadrature variance of ω and a beam splitter of transmissivity τ. In fact, the quadrature variance of $\hat{\rho}_{E_1E_2}$ and the transmissivity of the beam splitter in Fig. 14 are tuned in order to inject the same noise and to impose the same attenuation as in the original channel, respectively. In this beam splitter Eve combines the signal mode gleaned from Alice (mode B) with one mode (mode E_1) of the TMSV state. The first output of the beam splitter (mode B') which is the quantum signal received by Bob is given by $\hat{q}_{B'} = \sqrt{\tau}\hat{q}_B + \sqrt{1-\tau}\hat{q}_{E_1}$, and $\hat{p}_{B'} = \sqrt{\tau}\hat{p}_B + \sqrt{1-\tau}\hat{p}_{E_1}$. The second output of the beam splitter (mode E'_1) and mode E_2 of the TMSV state $\hat{\rho}_{E_1E_2}$ are stored by Eve in a quantum memory. Once the classical post-processing over the public channel is completed, this quantum memory is detected by means of an optimal joint measurement which estimates Alice's data (in direct reconciliation) or Bob's data (in reverse reconciliation). Note that in a Gaussian CV-QKD protocol, the asymptotic key rate against optimal collective Gaussian attacks can be calculated through the equivalent EB scheme based on the covariance matrix of the two-mode entangled state shared between Alice and Bob before their detection observations [87], [135], [136].

V. Free-Space Channels to and From Satellites

A. Sources of Loss in FSO Channels

The main sources of loss in FSO communication are diffraction, absorption, scattering and atmospheric turbulence [144]–[148], as encapsulated in Fig. 15. As will be discussed in this section, Diffraction-induced beam-spreading and turbulence-induced beam-wandering as well beam-spreading are dominant in good weather conditions, while absorption, scattering and scintillation are known to be relatively minor issues in good weather conditions.

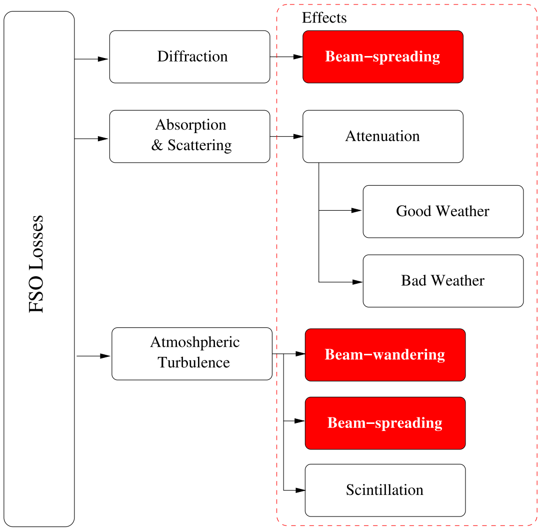


Fig. 15. Sources of losses in FSO channels and their effects on optical signal. Diffraction-induced beam-spreading and turbulence-induced beam-wandering as well beam-spreading dominate in good weather conditions.

Diffraction: Diffraction is a ubiquitous form of the natural wave propagation phenomenon experienced by light beams, and leads to beam-spreading (beam-broadening). Consequently, a certain fraction of the transmitted beam may not be collected by the receiver, since the diameter of the received beam is longer than the receiver's aperture, hence resulting in divergence loss, which increases upon increasing the length of the link. This loss may be mitigated by increasing the receiver's aperture as well as by reducing the transmission wavelength. However, a suitable compromise between the divergence loss, receiver size and cost as well as other transmission losses must be struck. Furthermore, a narrow beam is desirable to reduce diffraction losses, but this makes the link more sensitive to any misalignment between the transmitter and receiver.

Absorption and scattering: Absorption and scattering are imposed by the constituent gases and particles of the atmosphere. Both absorption as well as scattering impose attenuation on an optical wave. Explicitly, absorption is the phenomenon where the energy of optical wave is absorbed by the atmospheric particles, while scattering results in redistribution of the optical energy in arbitrary directions. Furthermore, both effects are strongly wavelength-dependent and become more pronounced when the transmission wavelength is comparable to the size of the atmospheric particles. Both scattering and absorption can be neglected, since they can be substantially mitigated by an appropriate choice of the communication wavelength. Explicitly, there is a negligible absorption at the visible wavelengths spanning from 0.4 to 0.7 mm. For these reasons, scattering and absorption was also neglected in [18], [54], [100]–[102], [110], and [149]–[151]. However, adverse weather conditions, for example fog, rain and snow,

[19] Gaussian collective attacks are as strong as coherent attacks in the limit of an infinite number of quantum states exchanged, however, it is not known this is the case for a realistic finite-length key protocols.

may severely limit the transmissivity of atmospheric channels, as discussed below:

- Fog includes particles having dimensions comparable to the transmission wavelength, hence it is the main source of atmospheric absorption and scattering. More specifically, dense fog may ultimately make optical transmission infeasible [152]. The impact of fog is generally quantified in terms of atmospheric visibility and the associated attenuation per unit length in dB/km. Explicitly, visibility is defined as the distance traversed by a parallel beam of light until its intensity drops to 2% of the original value [153], while the specific attenuation of fog in dB/km, denoted as α_{fog}, may be represented using the popular empirical Mie scattering model [147]:
$$\alpha_{\text{fog}}(\lambda) = \frac{3.91}{V}\left(\frac{\lambda}{550}\right)^{-p}, \tag{29}$$
where *V* is the visibility range in km, λ is the operating wavelength (550 nm is used as a reference wavelength for visibility range) and *p* is the size distribution coefficient of scattering obtained from the Kim or Kruse model [153]. Specifically, the Kim model gives [154]:
$$p = \begin{cases} 1.6 & V > 50 \\ 1.3 & 6 < V < 50 \\ 0.6V + 0.34 & 1 < V < 6 \\ V - 0.5 & 0.5 < V < 1 \\ 0 & V < 0.5, \end{cases} \tag{30}$$
while the Kruse model gives [155]:
$$p = \begin{cases} 1.6 & V > 50 \\ 1.3 & 6 < V < 50 \\ 0.585V^{\frac{1}{3}} & V < 0.6. \end{cases} \tag{31}$$
- From the detrimental effects of fog, rain and snow, rain has the least impact, because the size of rain droplets is large as compared to the transmission wavelength. The specific attenuation due to rain my be predicted using [147]:
$$\alpha_{\text{rain}} = k_1 R^{k_2}, \tag{32}$$
where R is the rain rate in mm/hr, while k_1 and k_2 are modeling parameters, whose value depends on both the size of rain droplets and on the temperature.
- The attenuation due to snow is higher than that of rain, but less than that of fog. However, heavy snow may severely reduce the link's availability, making it comparable to that of fog. The specific attenuation of snow is given by [147]:
$$\alpha_{\text{snow}} = aS^b, \tag{33}$$
where *S* is the snow rate in mm/hr, while the constants *a* and *b* are set to:
$$a = 5.42 \times 10^{-5} + 5.49, \quad b = 1.38 \tag{34}$$
in dry snowy conditions and to:
$$a = 1.02 \times 10^{-4} + 3.78, \quad b = 0.72 \tag{35}$$
in wet snowy conditions.

Hence, adverse weather conditions may significantly attenuate the optical signal, hence substantially degrading the availability of the FSO link. The transmission wavelength should be judiciously chosen to minimize these losses. Furthermore, sufficient link margin should be maintained for the sake of enhancing the link's availability.

Atmospheric turbulence: Atmospheric turbulence arises due to random fluctuations in the refractive index caused by stochastic variations of temperature. The atmosphere contains turbulent random inhomogeneities of various scales - also referred to as turbulent eddies [145]. They range from a large-scale (the outer scale of turbulence) to a small-scale (the inner scale of turbulence). These eddies affect optical wave-propagation through the atmosphere in different ways, depending on their size. In general, large scale eddies produce refractive effects and hence predominately distort the phase of the propagating wave, while small scale eddies are mostly diffractive in nature and therefore distort the amplitude of the wave [144], [145]. The most important effects resulting from the atmospheric eddies are beam-wandering, beam-spreading and beam-scintillation [144]–[146], [148]. We describe each of these three effects in more detail: (i) Random deviation of the beam from its original path is referred to as beam-wandering, which is caused by large-scale turbulent eddies, whose size is large compared to the beam-width. Beam-wandering causes time-varying power fades [54], [145], [146], [148]. (ii) Atmospheric turbulence results in a randomly fluctuating beam-width in the receiver's aperture plane. The broadening of the beam-width (when averaged over time) beyond that due to diffraction is termed as turbulence-induced beam-spreading [54], [57], [101], [145], [148], [156]. (iii) We define scintillation by fluctuations in the received irradiance (intensity) within the beam's cross section. Scintillation includes the temporal variation in the received irradiance and spatial variation within the receiver's aperture. Scintillation is mainly caused by small-scale turbulent eddies [144]–[146], [148].

B. Sources of Loss in FSO Channels to and From Satellites

In satellite-based quantum communications, the uplink and downlink channels are very different, since the atmospheric turbulence layer only occurs near the transmitter on an uplink, and only near the terrestrial receiver on a downlink. In the following, we briefly highlight how these two channels are affected by the above-mentioned turbulence-induced effects.

Uplink channels: For typical dimensions of the aperture size embedded in the ground station, the uplink optical beam first propagates through the turbulent atmosphere and its beam-width is much narrower than the size of the large-scale turbulent eddies [54], [145], [146], [148]. This makes beam-wandering the dominant effect in the uplink [54], [145], [146], [148]. Turbulence-induced beam-spreading also occurs to some extent in the uplink [54], [145]. As a result, the beam received by the satellite (when averaged over time) is wider than that associated with diffraction [54], [145]. Fig. 16 illustrates these two atmospheric effects, namely beam-wandering

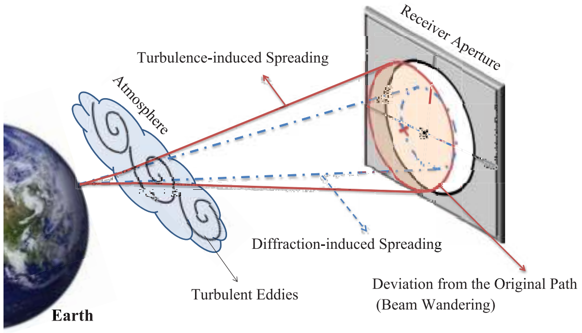

Receiver Aperture
Turbulence-induced Spreading
Atmosphere
Diffraction-induced Spreading
Turbulent Eddies
Deviation from the Original Path
(Beam Wandering)
Earth

Fig. 16. Illustration of beam-wandering (i.e., random deviation of the beam from its original path) and beam-spreading (including spreading induced by diffraction and spreading induced by turbulence) in uplink channels.

and beam-spreading in the uplink. Scintillation is not dominant in the uplink [145], [148].

Downlink channels: In contrast to the uplink case, the downlink optical beam propagates through the turbulent atmosphere only in the final part of its path. Considering the typical aperture size of the optical system embedded in the satellite, the beam-width at its entry into the atmosphere is likely to be larger than the scale of the turbulent eddies. As such, beam-wandering in the downlink tends to be less important relative to uplink channels [54], [145], [146], [148]. The photonic losses in the downlink are likely to be dominated by diffraction effects [54], [57]. Scintillation can occur to some extent in the downlink [145], [148]. However, as a consequence of aperture averaging, the downlink scintillation effects imposed on the detector tend to be negligible, when the receiver includes a large-diameter (>0.5 m) telescope [144], [145], [148].

C. Atmospheric Fading Channels

In atmospheric channels the transmissivity, η_t, fluctuates due to turbulence-induced effects. These fading channels can be characterized by the probability distribution of the transmission coefficients, η (where $\eta = \sqrt{\eta_t}$), which is denoted by $p(\eta)$. For a fading channel associated with the probability distribution $p(\eta)$ the mean fading loss in dB is given by $-10\log_{10}(\int_0^{\eta_0} \eta^2 p(\eta)\, d\eta)$, where η_0 is the maximum value of η.

As discussed in Section V-B, beam-wandering is the dominant turbulence-induced effect in the uplink. As an aside, we note that beam-wandering is expected to dominate the fading contributions in many terrestrial atmospheric communication scenarios [100], [102], [110], [111], [150].

D. Beam-Wandering Model

Here, we describe the probability distribution of the channel coefficients when the channel effects are dominated by beam-wandering. In the first instance we will assume that the beam-width at the receiver's aperture is fixed. That is, initially we will ignore any fluctuations in the beam-width caused by atmospheric turbulence.

In practice, beam-wandering causes the beam-center to be randomly displaced (along the *x* and *y* coordinates) from the center of the receiver's aperture plane. More explicitly, the beam's center position (x_l, y_l) randomly fluctuates around a fixed point, (x_d, y_d), hence its two-dimensional Gaussian distribution is given by [100]

$$p(x_l, y_l) = \frac{1}{2\pi\sigma_b^2} \exp\left(-\frac{(x_l - x_d)^2 + (y_l - y_d)^2}{2\sigma_b^2}\right), \quad (36)$$

where σ_b is the beam-wandering standard deviation. Thus, the beam-deflection distance, $l = \sqrt{x_l^2 + y_l^2}$, i.e., the distance between the beam-center and the aperture-center at (0, 0) fluctuates according to the Ricean distribution [100]

$$p(l) = \frac{l}{\sigma_b^2} I_0\left[\frac{ld}{\sigma_b^2}\right] \exp\left(-\frac{l^2 + d^2}{2\sigma_b^2}\right), \quad (37)$$

where $d = \sqrt{x_d^2 + y_d^2}$ is the distance between the aperture-center and the fluctuation-center (x_d, y_d), while $I_0[.]$ is the modified Bessel function. Note that $d = 0$ means that the beam-center fluctuates around the aperture-center. In beam-wandering the channel transmission coefficient, η, is a function of the beam-deflection distance, *l*, and is given by [100]

$$\eta^2 = \eta_0^2 \exp\left(-\left(\frac{l}{S}\right)^{\gamma}\right), \quad (38)$$

where γ is the shape parameter, *S* is the scale parameter and η_0 is the maximum value of η. The latter three parameters are given by

$$\gamma = 8h \frac{\exp(-4h) I_1[4h]}{1 - \exp(-4h) I_0[4h]} \left[\ln\left(\frac{2\eta_0^2}{1 - \exp(-4h) I_0[4h]}\right)\right]^{-1},$$
$$S = \beta \left[\ln\left(\frac{2\eta_0^2}{1 - \exp(-4h) I_0[4h]}\right)\right]^{-(1/\gamma)},$$
$$\eta_0^2 = 1 - \exp(-2h), \quad (39)$$

where $I_1[.]$ is the modified Bessel function, and where $h = (\beta/W)^2$, with β being the receiver's aperture radius and *W* the beam-spot radius at the receiver's aperture. Note that both β and *W* have the same units (meter). A schematic illustration of beam-wandering is shown in Fig. 17. According to Eqs. (37) and (38), the probability distribution $p(\eta)$ can be described by the log-negative Weibull distribution [100]

$$p(\eta) = \frac{2S^2}{\sigma_b^2 \gamma \eta} \left(2 \ln \frac{\eta_0}{\eta}\right)^{\left(\frac{2}{\gamma} - 1\right)} I_0\left[\frac{Sd}{\sigma_b^2} \left(2 \ln \frac{\eta_0}{\eta}\right)^{\frac{1}{\gamma}}\right]$$
$$\times \exp\left(\frac{-1}{2\sigma_b^2}\left[S^2 \left(2 \ln \frac{\eta_0}{\eta}\right)^{\frac{2}{\gamma}} + d^2\right]\right) \quad (40)$$

for $\eta \in [0, \eta_0]$, with $p(\eta) = 0$, otherwise. In some of the earlier literature, e.g., [157], the log-normal distribution was used. However, at the time of writing we are aware that the log-negative Weibull distribution more accurately describes the operationally important distribution tail [100]. In Fig. 18 the log-negative Weibull distribution is shown for fixed values of the beam-wandering standard deviation σ_b and the receiver's aperture radius β, and for different values of the beam-spot radius at the receiver's aperture *W* (the mean fading loss increases with increasing *W*). In Fig. 19 the log-negative

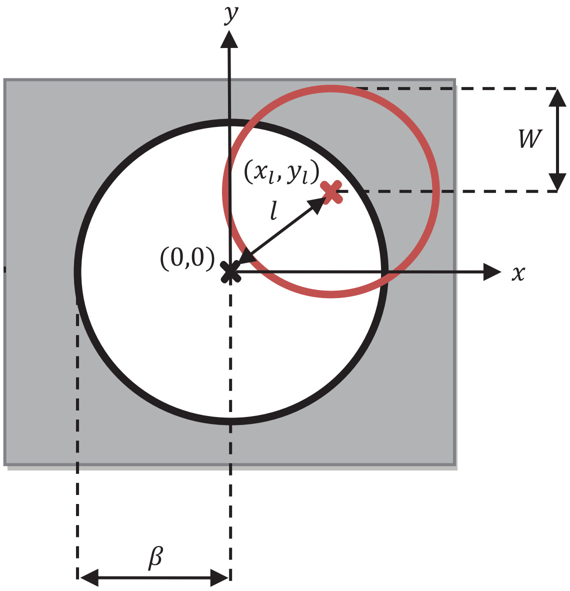


Fig. 17. A schematic illustration of beam-wandering in the receiver's aperture plane, where the beam-center (x_l, y_l) is randomly displaced (along the *x* and *y* coordinates) from the center of the receiver's aperture plane located at (0, 0).

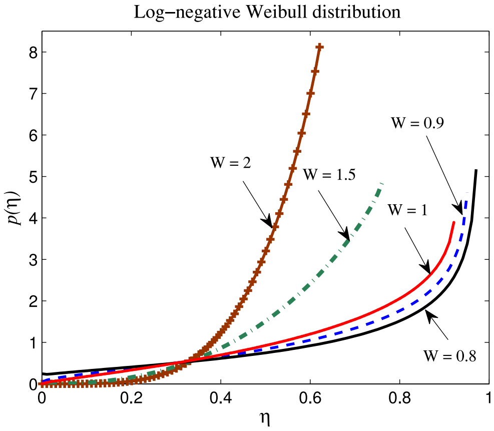


Fig. 18. The log-negative Weibull distribution for $\sigma_b = 0.7$, $\beta = 1$, and $d = 0$ with different values of *W*. For these parameters, $W = 0.8$ leads to a mean fading loss of 2.7 dB and $W = 2$ leads to a mean fading loss of 5.5 dB.

Weibull distribution is shown for the fixed values of W and β, with different values of σ_b (the mean fading loss increases with increasing σ_b).

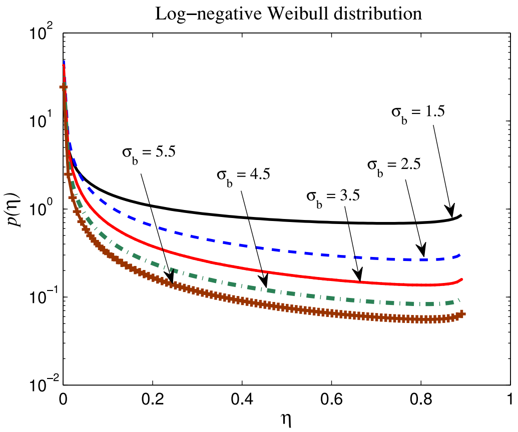


Fig. 19. The log-negative Weibull distribution for $W = 1.1$ and $\beta = 1$, and $d = 0$ with different values of σ_b. For these parameters, $\sigma_b = 1.5$ leads to a mean fading loss of 7.4 dB and $\sigma_b = 5.5$ leads to a mean fading loss of 17.8 dB.

Let us now we analyse the influence of beam-width fluctuations (caused by atmospheric turbulence) on the beam-wandering model just given. We refer to this effect as turbulence-induced beam-spreading. In doing this analysis, we will assume beam deformation does not occur - meaning the beam shape remains circular as it traverses the atmospheric channel (beam-deformation has been analysed in [101]). In turbulence-induced beam-spreading, the beam-spot radius W randomly changes in the receiver's aperture plane [101] with the probability distribution $p(W)$. Including this effect in our beam wandering model, the transmission coefficient of the channel, η, is now a function of the two random variables l and W according to Eqs. (38) and (39). We define a new variable Θ by setting $\Theta = 2\ln(\frac{W}{w_0})$, where w_0 is the initial beam-spot radius at the radiation source. This is useful since Θ randomly changes according to a normal distribution with the mean value $\langle\Theta\rangle$ and standard deviation σ_Θ [101]. Hence we have

$$p(\Theta) = \frac{1}{\sqrt{2\pi\sigma_\Theta^2}} \exp\left(-\frac{(\Theta - \langle\Theta\rangle)^2}{2\sigma_\Theta^2}\right). \tag{41}$$

With the inclusion of beam-width fluctuations in beam wandering, the calculation of a closed-form solution for $p(\eta)$ is not straightforward. However, given the knowledge of the probability distribution of $p(l)$ of Eq. (37) and $p(\Theta)$ of Eq. (41), we can calculate certain important quantities after averaging over all values of the channel's transmission coefficient. For instance, the mean fading loss in dB of a fading channel with the inclusion of beam-width fluctuations is now given by $-10\log_{10}(\int \eta^2(l,\Theta)p(l,\Theta)dld\Theta)$. Assuming that atmospheric turbulence is isotropic [101] and $d = 0$, the mean fading loss in dB of a fading channel (after the inclusion of beam-width fluctuations in the beam-wandering model) is given by $-10\log_{10}(\int \eta^2(l,\Theta)p(l)p(\Theta)dld\Theta)$. Note, with the inclusion of beam-width fluctuations, the maximum value of the channel's transmission coefficient η_0 is no longer fixed but rather randomly changes.

Optical losses in the downlink are usually orders of magnitude lower relative to uplinks [40], [66]–[68]. This means that if the "price" is paid in terms of placing the critical quantum technology on board the satellite (rather than the easier case of maintaining the quantum technology in ground stations), then much better quantum communication channels can be obtained. As alluded to earlier, the principal reason for this improvement is that in the downlink, diffraction of the beam is the main contributor to photon losses - not beam-wandering as in the uplink (see Fig. 20). The important fact is that by the time the downward-link beam hits the main turbulence-inducing layers of the atmosphere (this layer commences at about 20 km from ground level) the beam is much closer to its target and therefore any induced beam-wandering is less effective. Clearly, as opposed to most communication channels, there will be no directional reciprocity in channel

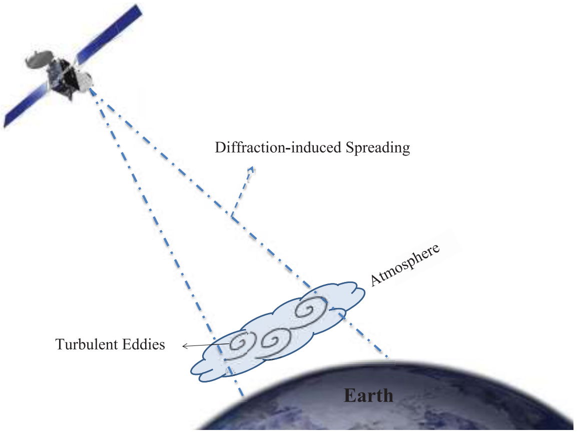


Fig. 20. Illustration of diffraction-induced beam-spreading as the main contributor to photon losses in downlink channels.

throughput for quantum communications with satellites. The recent experimental deployments of quantum communication in space have mostly exploited the more favourable downlink channel conditions [66], [67]. The losses in the downlink can then be modelled quite simply (to first order) through diffraction-only effects with the beam divergence following a λ/D scaling, where D is the diameter of the satellite telescope and λ is the transmission wavelength [40].

E. Estimation of a FSO Channel

Note that the rate of atmospheric fluctuations we consider are on the order of a few kHz, which is at least a thousand times slower than the typical transmission rates [145]. This means that the channel's transmission coefficient can be measured at the cost of additional (classical) transmission and receiver complexity [17], [149], [150], [158]. These channel measurements may be carried out using several schemes, e.g., by transmitting coherent (classical) light pulses that are intertwined with the quantum information [149], [150] or by transmitting a local oscillator (i.e., a strong coherent laser pulse which is mixed with the signal field in the homodyne detection and serves as a phase reference) [17]. In [17] measurement of the atmospheric channel's transmission coefficients was carried out in real time at the receiver by passing a local oscillator through the channel in a mode orthogonally polarized to the signal. The technique of measuring the atmospheric channel's transmission coefficient by an auxiliary classical laser beam was introduced in 2012 [149], and its practical employment was demonstrated for a one-way communication link in 2015 [150]. The same technique based on the intensity of the signal itself was realized in [158].

VI. Entanglement Distribution and CV-QKD Implementation Via Satellite

A. Entanglement Distribution and Standard QKD Protocols

In the context of satellite-based quantum communication we are faced with two different channels, namely, the uplink (ground-to-satellite) channels and the downlink (satellite-to-ground) channels. In the uplink, the ground station transmits signals to the satellite receiver, and in the downlink, the satellite transmits signals to the ground station receiver. Correspondingly, there are several possible architectures for implementing satellite-based quantum communication depending on the types of links utilized. Some of these configurations are illustrated in Fig. 21. Explicitly, the schemes (a) and (b) illustrate the uplink and downlink channels, respectively (both links have been demonstrated in the DV domain [65], [66], [68]). In scheme (c) of Fig. 21, the deployment of quantum technology at the satellite is minimized, since the satellite is utilized only in a reflector mode (i.e., a simple relay). As a proof of concept for the reflecting paradigm, we note the recent experimental tests of [47]–[49], where single photons (weak laser coherent pulses) emitted by the ground station were reflected (and subsequently detected on the ground) by a LEO satellite via the satellite's cube retroreflectors. In scheme (c) the complex quantum engineering components are limited to the ground stations, since the source of quantum states is located in one of the ground stations and the receiver of quantum states is located in the other ground station. Although satellite reflection towards another station

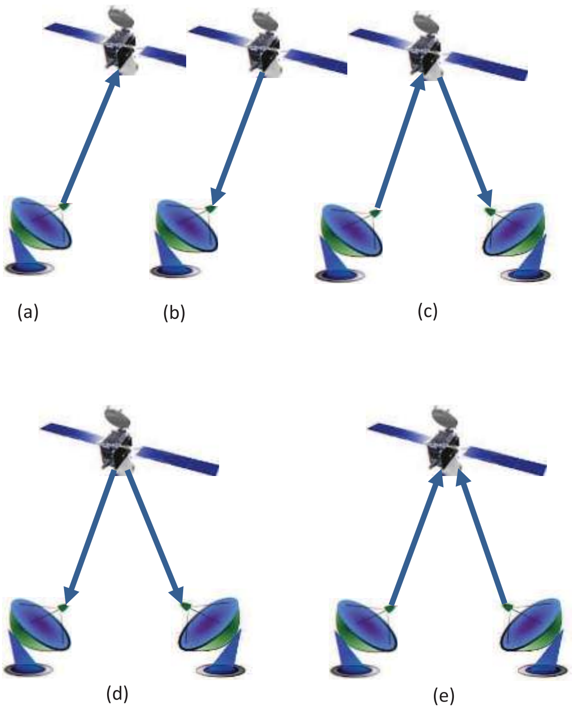


Fig. 21. Illustration of various architectures for implementing satellite-based quantum communication. In (a) ((b)) quantum states are transmitted from the ground station (satellite) to the satellite (ground station) over an uplink (a downlink) channel. In (c) quantum states are transmitted from one ground station over an uplink channel to the satellite, and then reflected at the satellite to the second ground station over a downlink channel. In (d) quantum states are generated on board the satellite, and then transmitted through different downlink channels to separate ground stations. In (e) quantum states are transmitted from two separate ground stations over two different uplinks to the satellite, at which quantum measurements are performed on the received quantum states, and the classical measurement results are communicated back to the ground stations.

constitutes a sophisticated engineering task in its own right, it does not require onboard generation of quantum communication information. There are many practical advantages in deploying quantum communication technology at the ground stations, such as lower-cost maintenance, and the ability to rapidly upgrade as new quantum technology matures. The other schemes, (d) and (e), in Fig. 21 can be considered as space-based high-complexity schemes, since they involve the deployment of quantum technology at the satellite. In scheme (d) (again already demonstrated for DV states [67]) the source of quantum states is located on board the satellite, with both ground stations acting as receivers. In scheme (e) the two ground stations transmit quantum states to the satellite. In the satellite, quantum measurements are performed on the received states and the classical measurement results are communicated back to the ground stations. Scheme (e) can be utilized in support of entanglement swapping and measurement-device-independent protocols so as to implement QKD between the two ground stations.

Let us reconsider the quantum communication architectures of Fig. 21 for CV entanglement distribution and for CV-QKD implementation. We assume that the source of quantum communication in the transmitter(s) is a two-mode entangled state associated with modes 1 and 2. In the scheme (a) (the scheme (b)) of Fig. 21, a two-mode entangled state is generated by Alice at the ground station (satellite) with one mode, mode 1, kept by Alice, while the other mode, mode 2, is transmitted to Bob located at the satellite (ground station) over the uplink (downlink). In the scheme (c) of Fig. 21, a two-mode entangled state is generated by Alice at the ground station transmitter with one mode, mode 1, held at the ground station transmitter and the other mode, mode 2, transmitted over the uplink to the relay satellite. The received mode is then reflected in the satellite and transmitted through the downlink to Bob at the ground station receiver. In the scheme (d) of Fig. 21, a two-mode entangled state is generated on board of the satellite with both modes then sent over the separate downlinks to Alice and Bob located at the separate ground stations. In the scheme (e) of Fig. 21, Alice and Bob are located in the separate ground stations, both initially possessing a two-mode entangled state. One mode of each entangled state is kept by a ground station transmitter and the second mode of each state is transmitted over the uplink to the relay satellite, in which on-board entanglement swapping is performed on the arriving modes. To elaborate a little further, entanglement swapping [7] is a standard quantum protocol conceived for establishing entanglement between distant quantum systems that have never interacted [159]–[162]. It is the central mechanism of quantum repeaters [31], enabling the distribution of entanglement over large distances. In the scheme (e) of Fig. 21, the received modes are swapped at the satellite via a CV Bell measurement [82], where the two modes are mixed through a balanced beam splitter. Explicitly, the $\hat{q}$ quadrature of one of the output modes of the beam splitter and the $\hat{p}$ quadrature of the output mode are separately measured by two homodyne detectors. This process is sometimes described by saying that the two output modes of the beam splitter are conjugately homodyned [82]. The classical outcome of the Bell measurement is then communicated to Alice and Bob so that they can optimally displace their modes, according to the measurement outcome, in order to maximize the resultant entanglement shared between the ground stations. This entanglement swapping scheme between two ground stations via satellite is shown more explicitly in Fig. 22.

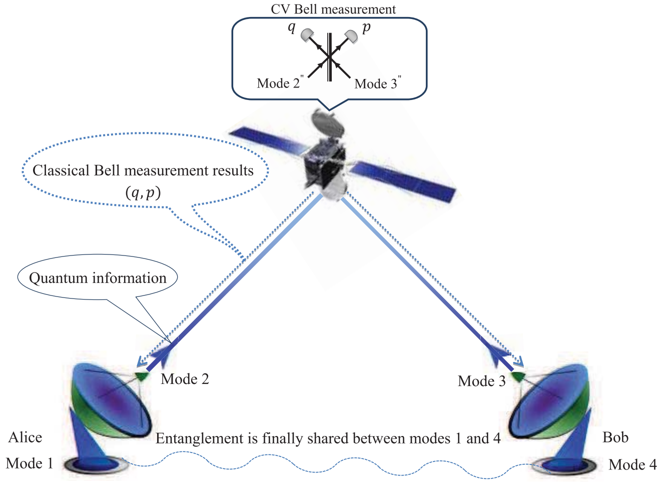


Fig. 22. Entanglement swapping between two ground stations via satellite: The two-mode entangled state of modes 1 and 2 (modes 3 and 4) is initially owned by Alice (Bob). Mode 1 (mode 4) is kept by Alice (Bob) and mode 2 (mode 3) is then transmitted over the uplink to the relay satellite. The received modes $2''$ and $3''$ (where the $''$ indicates that the modes have now incurred losses) are mixed through a balanced beam splitter and the $\hat{q}$ quadrature of one of the output modes and the $\hat{p}$ quadrature of the other one are measured by two homodyne detectors. The classical outcome of the Bell measurement is then communicated to Alice and Bob. As a result, there would exist an entangled state shared between modes 1 and 4.

As a result of the entanglement distribution in each quantum communication scheme of Fig. 21, there would exist an entangled state shared between Alice and Bob. Once the entangled states have been shared between the stations, for each scheme of Fig. 21, Alice and Bob are able to invoke CV-QKD protocols in the EB scheme by applying homodyne or heterodyne detection of their own modes. The level of entanglement produced by the quantum communication schemes considered here as well as the quantum key rates of the EB CV-QKD protocols in these schemes have recently been analyzed in [105]–[109].

In the schemes (a), (b), and (c) of Fig. 21 the entangled source originates from one of the trusted parties (Alice). However, in the scheme (d) of Fig. 21 the entangled source originates from the satellite, which in some circumstances may be controlled by the eavesdropper, Eve. In [136], it has been shown that in the context of the EB CV-QKD protocols Alice and Bob can still generate a secure key, even when Eve controls the entanglement source.

B. Measurement-Device-Independent QKD Protocols

In the scheme (e) of Fig. 21 the entangled source originates from both trusted parties (Alice and Bob), however, the Bell measurement at the satellite may be controlled by

Eve. In [163], it has been demonstrated that in CV-QKD protocols the secret key to be shared between the two trusted parties can be generated by the measurement of an untrusted intermediate relay. In measurement-device-independent (MDI) protocols of QKD [163]–[165], Alice and Bob are not connected by direct links, and an intermediate relay is used for completing the communication link. In MDI protocols the measurement device is the intermediate relay, whose operation may be controlled by an adversary. Fig. 22 is in fact one example of a scenario over which a MDI protocol may be implemented.

The security of CV-MDI protocols is usually analysed using EB schemes that invoke CV entanglement swapping at the relay similar to that shown in Fig. 22 Although CV-MDI protocols are practically implemented in a PM scheme (see below).

In the EB equivalent of the Gaussian MDI-QKD protocols, a pair of TMSV states associated with the quadrature variance of $v = \cosh(2r)$ (where r is the two-mode squeezing), is initially owned by Alice and Bob. One mode of each entangled state is held by Alice and Bob, while the second mode of each state is transmitted to the intermediate relay over the insecure channel. The received modes are swapped via a CV Bell measurement at the intermediate relay. The swapping process continues by the relay communicating the Bell measurement result through a classical public channel to Alice and Bob. After receiving the Bell measurement outcome, Bob displaces his mode, while Alice keeps her mode unchanged. Then Alice and Bob measure their modes by homodyne (or heterodyne) detectors to create correlated data. After the establishment of a sufficiently large amount of correlated data, Alice and Bob proceed with the classical post-processing over an authenticated public channel to create a secret key.

In the EB scheme of the Gaussian MDI-QKD protocols, if Alice and Bob apply a homodyne detection of their modes, the scheme becomes equivalent to the PM scheme, in which Alice and Bob prepare squeezed states, and if Alice and Bob apply a heterodyne detection of their modes, the scheme becomes equivalent to the PM scheme in which Alice and Bob prepare coherent states. We discus these PM schemes next.

The MDI implementation of Gaussian CV-QKD protocols in the PM scheme depends on whether the Gaussian resource is a squeezed or a coherent state. If a squeezed state, Alice prepares her mode in a squeezed state with the quadrature variance $v = \exp(2r_s)$, where r_s is the single-mode squeezing. Which one of the two quadratures is to be squeezed is based on a randomly generated bit. The chosen quadrature is then modulated by a random Gaussian-distributed variable with zero mean and variance v_m conditioned on $v_m = v - 1/v$. The same procedure is applied independently at Bob's side. If the Gaussian resource is a coherent state, Alice prepares her coherent-state mode with each quadrature independently modulated by a random Gaussian-distributed variable having zero mean and variance of v'_m. Likewise Bob.

Following transmission to the satellite of the modes belong to Alice and Bob, and irrespective of the Gaussian resource used, the satellite makes a CV Bell measurement on each mode pair, announcing the results. Alice and Bob undertake some modification of their data based on these results and undergo some classical post-processing to end up with a shared key. More details of this process can be found in [108].

Note the modulation variance v'_m (in the protocol using coherent states) can reach very high values, e.g., $v'_m = 60$ [163]. With the use of squeezed states, however, achieving high values of squeezing reamins experimentally challenging. As such, quadrature variance v and of the modulation variance v_m are limited in the range of values attained. Note that $v = 5.05$ is equivalent to the two-mode squeezing of 10 dB [166]. Note also that vacuum squeezing at 15 dB is currently the highest obtainable in any experiment [167].

Previous contributions on MDI-QKD protocols have mainly been focussed on fixed-attenuation channels [30], [163], [168]–[177]. In [108], a MDI implementation has been investigated in order to establish Gaussian CV-QKD protocols between two ground stations, where the communication occurs between the ground stations via a LEO satellite over a pair of independent atmospheric channels. In this CV-MDI protocol the measurement device is the satellite itself, which can be controlled by an adversary. In [108], it has been demonstrated that while the CV-MDI protocol is only feasible for low-loss fixed-attenuation channels, the protocol is capable of achieving a beneficial secure key rate even for transmission over high-loss atmospheric channels. Note that in MDI-QKD the devices of Alice and Bob have to be trusted [30], [163], [168]–[177]. Nonetheless, it has recently been shown that QKD is possible even when the device of one of the parties is untrusted [178]–[180]. The security of this one-sided device-independent protocol using CV quantum states has recently been investigated both theoretically and experimentally [181], [182].

We note that MDI protocols represent a step closer to full device-independent protocols. These latter protocols are based on Bell violation measurements at the receivers, and represent the most robust form of QKD (the form that requires the least number of assumptions). Although some work has been carried out in relation to CV states in device independent QKD (e.g., [183]), practical progress is limited due to the very low key rates expected. CV MDI-QKD protocols, with their reduced assumptions on how the measurement device must operate, currently represent the most robust form of QKD that still lead to reasonable key rates. The MDI protocols remain unconditionally secure in their generation of keys - the best an adversary in charge of the measurement device can do is drive the key rate to zero (e.g., by broadcasting false Bell measurement results).

C. Entanglement Determination and Quantum Key Rate Computation

The evolution of quantum states as they prorogate through atmospheric fading channels can be considered in two different scenarios. In the first scenario, the transmission coefficient η of the atmospheric fading channel is unknown, while in the second scenario it is known. In this latter scenario, it is assumed that the transmission coefficient can be measured in real time at the receiver.

1) Scenario 1 (The Transmission Coefficient of the Fading Channel Is Unknown): Here, we consider the distribution of a two-mode entangled state over satellite-based atmospheric fading channels. In fact, we assume that the transmitter initially possesses a two-mode (mode 1 and mode 2) entangled state $\hat{\rho}$, with one (or more) of the modes transmitted to the receiving station(s) through atmospheric fading channels. This leads to two operational settings.

Single-mode transfer: In this setting we assume that mode 1 of $\hat{\rho}$ remains at the ground station (satellite), while mode 2 of $\hat{\rho}$ is transmitted to the satellite (ground station) over the fading uplink (downlink) characterized by the probability distribution $p(\eta)$ and the maximum transmission coefficient of η_0. The density operator of the two-mode state at the ground station and satellite for each realization of the transmission coefficient η is given by $\hat{\rho}'(\eta)$. Since η is a random variable, the elements of the total density operator of the resultant mixed state $\hat{\rho}'_t$ are calculated by averaging the elements of the density operator $\hat{\rho}'(\eta)$ over all possible transmission coefficients of the fading channel, giving the ensemble-averaged state of [107]

$$\hat{\rho}'_t = \int_0^{\eta_0} p(\eta)\hat{\rho}'(\eta)\, d\eta. \tag{42}$$

Now, let us consider the initial two-mode entangled state $\hat{\rho}$ at the transmitter being a Gaussian state [102], [103], [105], [106], [184]. In this case the resultant ensemble-averaged state $\hat{\rho}'_t$ is a non-Gaussian mixture of the Gaussian states $\rho'(\eta)$ obtained for each realization of η. Since the resultant ensemble-averaged state shared by the ground station and the satellite is a non-Gaussian state, it cannot be completely described by its first and second moments. Therefore, the final entanglement computed based on the covariance matrix of the resultant ensemble-averaged state will represent only the Gaussian entanglement between the ground station and the satellite, but not the total distributed entanglement [102], [103], [105], [184]. In order to calculate the total shared entanglement between the stations, the entanglement has to be computed based on the density operator of the resultant ensemble-averaged state [107].

Note that if we use the shared entanglement created for subsequent use in QKD, i.e., a EB CV-QKD protocols operating over atmospheric fading channels,[20] then the same concept (use of ensemble averaged states) is invoked when the quantum key rate is calculated. Note that when the quantum key rate is in fact calculated based on the covariance matrix of the resultant ensemble-averaged state $\hat{\rho}'_t$, the key rate computed is only related to the Gaussian component of $\hat{\rho}'_t$ [106].

Two-mode transfer: In this setting we assume that the satellite initially possesses a two-mode entangled state $\hat{\rho}$, with mode 1 transmitted to ground station 1 over a fading downlink obeying the probability distribution of $p_1(\eta_1)$ and having the maximum transmission coefficient of η_{01}, while mode 2 is transmitted to ground station 2 over a different fading downlink characterized by the probability distribution $p_2(\eta_2)$ and having the maximum transmission coefficient of η_{02}. Here, the two fading downlinks are assumed to be independent. The density operator of the two-mode state at the ground stations for each realization of the transmission coefficients η_1 and η_2 is given by $\hat{\rho}'(\eta_1, \eta_2)$. The elements of the total density operator of the resultant mixed state $\hat{\rho}'_t$ are calculated by averaging the elements of the density operator $\hat{\rho}'(\eta_1, \eta_2)$ over all possible transmission coefficients of the two separate fading channels, giving the ensemble-averaged state of [107]

$$\hat{\rho}'_t = \int_0^{\eta_{01}} \int_0^{\eta_{02}} p_1(\eta_1)p_2(\eta_2)\hat{\rho}'(\eta_1, \eta_2)\, d\eta_1 d\eta_2. \tag{43}$$

2) Scenario 2 (The Transmission Coefficient of the Fading Channel Can Be Measured): Let us now assume a modified scenario, in which the variable transmission coefficient of the atmospheric fading channel is measured with the aid of a separate coherent signal. For example, when a local oscillator in a polarized mode orthogonal to the signal is sent through the channel. Although this increases the complexity of the system, the grade of entanglement (and hence the quantum key rate of the EB CV-QKD protocols implemented based on this entanglement) generated between the stations will be increased.

When considering this scenario in the single-mode transfer setting where the transmission coefficient η is measured at the receiving station, the final entanglement can be calculated as [107]

$$E = \int_0^{\eta_0} p(\eta)\, E\big[\rho'(\eta)\big]\, d\eta, \tag{44}$$

where $E[\rho'(\eta)]$ is the grade of entanglement of a state received through the channel of transmission coefficient η.

In this scenario, when the initial two-mode entangled state $\hat{\rho}$ at the transmitter is a Gaussian state, the mixed states $\rho'(\eta)$ collected at the receiver during each transmission coefficient window remain Gaussian, because within each (small) fading bin we can assume that the transmission coefficient is constant and therefore the states during that particular bin remain Gaussian. In this case, the grade of entanglement of the mixed Gaussian state $\rho'(\eta)$, i.e., $E[\rho'(\eta)]$ can be calculated based on the covariance matrix of $\rho'(\eta)$, which results in E of Eq. (44) representing the total entanglement shared between the stations [107].

Considering this scenario in the EB CV-QKD protocols communicating over atmospheric fading channels, which are implemented based on the shared entangled states between the stations, the same concept is true when the quantum key rate is calculated. In fact, due to the relatively long coherence time of the atmospheric channel, it may be possible to devise a scheme, in which quantum key rates are derived for each realization of the fading (each fading bin realized), and summed [107]–[109], [186]. Indeed, the quantum key rate $K[\rho'(\eta)]$ resulting from the mixed Gaussian state $\rho'(\eta)$ can be calculated based on the covariance matrix of $\rho'(\eta)$, and then the total key rate shared between the stations is calculated by $K = \int_0^{\eta_0} p(\eta)\, K[\rho'(\eta)]\, d\eta$ [107]–[109].

[20] Note that in [185], a fast-fading channel has been considered where the users are only able to estimate the probability distribution of the channel's transmission coefficient but not its instantaneous values, while the eavesdropper has full control of the fast-fading channel, so that she chooses the instantaneous transmission coefficient of the channel.

Similarly, considering this scenario in the two-mode transfer setting, where the transmission coefficients η_1 and η_2 are measured at the two receiving stations, the final grade of entanglement can be calculated as [107]

$$E = \int_0^{\eta_{01}} \int_0^{\eta_{02}} p_1(\eta_1) p_2(\eta_2) E[\hat{\rho}'(\eta_1, \eta_2)]\, d\eta_1 d\eta_2, \quad (45)$$

where $E[\hat{\rho}'(\eta_1, \eta_2)]$ is the entanglement of a state that has traversed two channels having the transmission coefficients of η_1 and η_2 [107]–[109].

D. Enhancement of Quantum Communication Performance

Satellite-based communication channels tend to suffer from high uplink losses on the order of 25-30 dB (and beyond) for a LEO satellite receiver [40], [52], [145], while single downlink channels are anticipated to have losses of 5-10 dB for a LEO satellite transmitter [40], [52], [145]. Under such high losses, entanglement distribution and QKD via satellite will remain a fruitless endeavor without the beneficial intervention of the post-selection strategy [102] and entanglement distillation techniques [184] detailed below.

1) Post-Selection: Although atmospheric fading degrades both the entanglement and the quantum key rate, its effects may be mitigated. Post-selection of high transmission-coefficient windows, as introduced in [102] for the case of a single point-to-point fading channel, is capable of improving both the entanglement and the quantum key rate. To elaborate a little further, in the post-selection strategy, a subset of the channel transmittance distribution, namely that associated with the high transmission coefficient, is selected to contribute to the resultant post-selected state and to the post-selected key rate.

To elaborate on the post-selection strategy, in addition to the quantum states, coherent (classical) light pulses are transmitted through the channel in order to estimate the channel's transmission coefficient η at the receiver. The received quantum state is either retained or discarded, conditioned on the channel's transmission coefficient being higher or lower than the post-selection threshold η_{th}. Although this post-selection strategy can be invoked for enhancing the grade of entanglement and the quantum key rate between the transmitter and receiver, estimation of the channel's transmission coefficient will impose additional complexity on both the transmitter and receiver. The operation of this form of post-selection in the scheme (c) of Fig. 21 has been invoked in [105] for enhancing the grade of Gaussian entanglement and in [106] for increasing the quantum key rates between the ground stations.

2) Entanglement Distillation: The other strategy, which can be used in order to enhance the grade of entanglement between the transmitter and receiver is entanglement distillation that is based on quantum measurement techniques without relying on channel estimation. Entanglement distillation represents the protocol of extracting a subset of states with a higher degree of entanglement from an ensemble of entangled states [187]. In fact, entanglement distillation may be viewed as a purifying protocol that selects highly entangled pure states from a set of entangled states that have become mixed as a result of imperfect transmission [188]–[191]. It has been shown that if the entangled states are Gaussian, entanglement distillation cannot be performed using only Gaussian operations carried out by linear optical components, such as beam splitters and phase shifters, homodyne detection and classical communication [192]–[194]. However, when the Gaussian entangled states are transmitted through a fading channel, the state at the output of the channel is a non-Gaussian mixed state (a non-Gaussian mixture of Gaussian states), and therefore the aforementioned no-go theorem does not apply. In [184], a method has been proposed for distilling entanglement from (initially) Gaussian entangled states received over a single point-to-point fading channel. This is achieved by carrying out a weak measurement (based on a beam splitter and a homodyne detector) applied to the received non-Gaussian mixed state. The entanglement distillation is implemented at the receiver by extracting a small portion of the received mixed state using a tap beam splitter. A single quadrature (for instance, the $\hat{q}$ quadrature) is then measured by applying homodyne detection to the tapped beam. If the measurement outcome is above the threshold value q_{th}, then the remaining state is retained, otherwise it is discarded. The operation of this form of entanglement distillation in the scheme (c) of Fig. 21 has been invoked in [105] for enhancing the Gaussian entanglement between the ground stations (which consequently leads to an improvement in the quantum key rates of the EB CV-QKD protocols).

Note that when entangled states are conveyed over a fading channel, both the above-mentioned post-selection and entanglement distillation strategies act as "Gaussification" methods in the sense that the resultant conditioned states approach a Gaussian form due to the enhanced concentration of low-loss states in the final ensemble-averaged state. Note also that using the above-mentioned post-selection and entanglement distillation strategies, the entanglement established between the transmitter and receiver is only probabilistically increased.

Another entanglement distillation technique is based on applying an initial non-Gaussian operation to the Gaussian entangled states (that again increases the entanglement probabilistically), which is followed by a Gaussification step that iteratively drives the output non-Gaussian state towards a Gaussian state. Non-deterministic noiseless linear amplification has been identified as a method of distilling Gaussian entanglement [196] and [195], [197]–[203]. It has been shown that the non-deterministic noiseless linear amplification is capable of distilling improved CV entanglement [196], [199], [200] and enhancing CV-QKD performance [201]–[203], when applied after the lossy channel to the quantum states received. The non-Gaussian operations which result in the generation of non-Gaussian entangled states will be discussed in detail in the next section.

VII. Non-Gaussian CV Quantum Communication Over Atmospheric Channels

In the CV domain, previous efforts invested in entanglement distribution and QKD over atmospheric channels have been predominately focussed on Gaussian states [16], [98], [102], [103], [105], [106], [108], [110], [111]. Although Gaussian quantum states are well understood both from a theoretical and from an experimental perspective [86], [87], [114], the employment of CV non-Gaussian quantum states[21] for quantum communication has also garnered interest [204]–[224]. Non-Gaussian quantum states are valuable resource for a range of protocols, including teleportation [204]–[208], [212]–[214], cloning [222], [223] and CV-QKD protocols [219]–[221], [224]. For two important reasons, entangled non-Gaussian states are particularly interesting in the context of quantum communication via satellite. The first of these reasons is that the distillation of Gaussian entanglement is impossible using only Gaussian operations [192]–[194]. However, mixed non-Gaussian states can undergo entanglement distillation without any additional requirements. The second reason is that, relative to Gaussian entanglement, non-Gaussian entanglement can be shown in some circumstances to be more robust against decoherence [212], [217], [218].

A. Non-Gaussian Entangled States

CV non-Gaussian states are mostly generated by applying non-Gaussian operations, such as photon subtraction [204], [205], [207]–[210], [213], [214], photon addition [206], [207], [209], [211], [214] and photon replacement [212], [214] to incoming Gaussian states. We discuss here non-Gaussian entangled states which are created probabilistically by applying non-Gaussian operations to (i.e., at the receiver) Gaussian TMSV states. Note that a non-Gaussian operation can be applied to either a single mode, or to both modes, of the incoming Gaussian entangled state. Also note the non-Gaussian operation can be applied to the incoming mode at the sender (i.e., incoming from the local TMSV production site), or at the receiver side (after propagation through the atmosphere). Unless otherwise stated, we will consider the former process in the following.

For the generation of an entangled photon-subtracted squeezed (PSS) state [204], [205], [207]–[210], [213], [214], each mode of an incoming TMSV state interacts with a vacuum mode in a beam splitter. One of the outputs of each beam splitter feeds a photon number resolving detector. When both detectors simultaneously register k photons, which are considered to be non-Gaussian measurements, a pure non-Gaussian state is heralded with a probability of $0 < P_{sb} < 1$. This photon-subtraction operation is shown in Fig. 23(a) for $k = 1$. A PSS state can also be generated by applying the photon subtraction technique described above to a single mode of the TMSV state [214]. The generation of non-Gaussian states via photon subtraction as described above has been experimentally demonstrated in [225]–[227]. Note that in the photon-subtraction operation, other types of photon detectors such as on/off photon detectors (which only distinguish the presence and absence of photons, and are considered a non-Gaussian measurement) can also be used for generating a PSS state from a TMSV state [205], [208]. In this case the non-Gaussian output state is a mixed state.

An entangled photon-added squeezed (PAS) state [206], [207], [209], [211], [214] is generated by adding a single photon to each mode of a TMSV state. This single-photon addition is performed at a beam splitter, as shown in Fig. 23(b), with one of the outputs of each beam splitter being detected by an on/off photon detector. A pure non-Gaussian state is then generated (with a probability of 0< P_{ab} <1) when a vacuum state is registered in both detectors simultaneously. Note that the final creation probability of a PAS state is obtained by multiplying P_{ab} by the probability of creating the two additional photons required. A PAS state can also be generated by applying the photon addition technique described above to a single mode of the TMSV state [214]. Note that the addition of single photons to coherent states and to thermal states of light has been experimentally realized in [228] and [229].

By contrast, an entangled photon-replaced squeezed (PRS) state [212], [214] is generated according to Fig. 23(c), where each mode of a TMSV state interacts with a single photon in a beam splitter, with one of the outputs of each beam splitter being detected by a photon number resolving detector. When both detectors register a single photon simultaneously, a pure non-Gaussian state is heralded with a probability of 0< P_{rb} <1. The final creation probability of a PRS state is obtained by multiplying P_{rb} by the probability of creating the two additional photons required. A PRS state can also be generated by applying the photon replacement process described above to a single mode of the TMSV state [214].

B. Evolution of Non-Gaussian Entangled States Over a Lossy Channel

Unlike Gaussian states, the evolution of non-Gaussian states cannot be analysed solely through the covariance matrix. Previous contributions have analysed the evolution of non-Gaussian states for transmission over fixed-attenuation channels relying on the so-called Master equation approach of [215], the characteristic function approach of [212] or the Kraus operator approach of [217]. Here we discuss the general approach of Kraus representation [230] of the channel in order to directly analyze the evolution of the entangled states (Gaussian or non-Gaussian) through the channel. Considering a quantum state associated with the density operator $\hat{\rho}_{in}$ as the input of a trace-preserving[22] completely positive channel, the output density operator of the channel can be described in an operator-sum representation of the form $\hat{\rho}_{out} = \sum_{\ell=0}^{\infty} G_\ell \hat{\rho}_{in} G_\ell^\dagger$, where the Kraus operators G_ℓ satisfy $\sum_{\ell=0}^{\infty} G_\ell G_\ell^\dagger = I$, with I being the identity operator. In [230], the Kraus operators of a wide range of channels including a fixed-attenuation channel subject to vacuum noise (i.e., $V_n = 1$ in Fig. 10) are given. In [217], the Kraus operators of a fixed-attenuation channel subject to vacuum noise but with additional Gaussian noise is given. The results of [230] have been generalized to a fixed-attenuation channel subject to thermal noise (i.e., $V_n > 1$ in Fig. 10) in [132].

[21] Note that only pure states having a positive Wigner function are Gaussian states. However, the Wigner function of non-Gaussian pure states takes on negative values.

[22] In a trace-preserving channel, the trace of the density operator is preserved, which means the trace of the output density operator of the channel remains one.

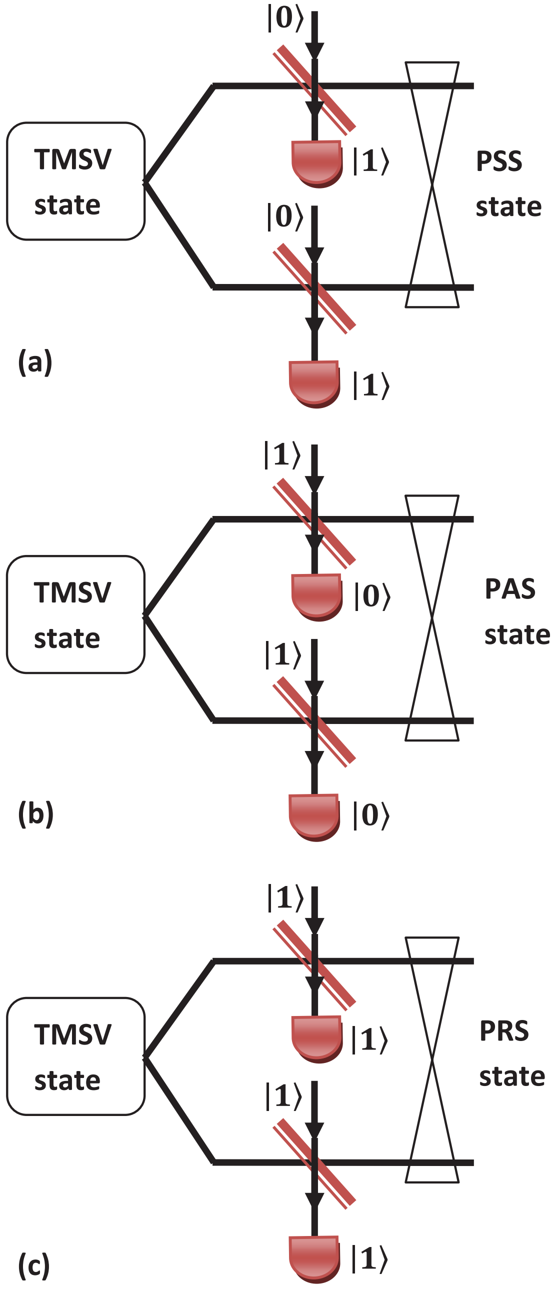


Fig. 23. Implementation of non-Gaussian operations on the Gaussian TMSV state. (a) Photon subtraction: each mode of the input TMSV state interacts with a vacuum mode in a beam splitter, with one output of the each beam splitter feeding a photon detector. If the two detectors simultaneously detect a single photon, a PSS state is heralded on the non-measured outputs. (b) Photon addition: each mode of the input TMSV state interacts with a single photon in a beam splitter, with one output of the each beam splitter feeding a photon detector. If the two detectors simultaneously detect vacuum state, a PAS state is heralded on the non-measured outputs. (c) Photon replacement: each mode of the input TMSV state interacts with a single photon in a beam splitter, with one output of the each beam splitter feeding a photon detector. If the two detectors simultaneously detect single photons, a PRS state is heralded on the non-measured outputs.

C. Entanglement Determination and Quantum Key Rate Computation

Following the evolution of pure non-Gaussian states over the lossy channel(s), the quantum state of the channel output is a non-Gaussian mixed state. In general it is not possible to analytically determine the total grade of entanglement of the mixed non-Gaussian states after transmission over a lossy channel. Since the grade of entanglement is determined by the output density operator $\hat{\rho}_{out}$, which possesses an infinite number of elements, a numerical method is required for approximating the matrix $\hat{\rho}_{out}$ by its truncated-dimensional version, as discussed in [107], [109], [132], and [205] whilst ensuring that the trace of the truncated matrix is close to 1.

Given the non-deterministic nature of the non-Gaussian operations, in the context of non-Gaussian entanglement distribution, there are two key performance indicators, namely the grade of entanglement E between two stations following the transmission of a pulse through the lossy channel(s), and the entanglement-generation rate R_E, where we have $R_E = P_c\, E$, with P_c being the creation probability of the initial non-Gaussian state. The evolution of a wide range of non-Gaussian entangled states in both single-mode and two-mode transfer over atmospheric fading channels has been investigated both when the transmission coefficient of the atmospheric fading channel is unknown and when it is estimated in real time [107]. The work of [107] considered operational scenarios where the non-Gaussian entangled states transmitted through the atmospheric channel are created "just-in-time" via non-Gaussian operations applied to the Gaussian entangled input states that would otherwise be transmitted directly over the communication channel. In this scenario transmitting the incoming Gaussian state directly over the atmospheric channel would be the best option in terms of maximizing the *entanglement-generation rate*. However, if the transmission rates of all the states through the channel could be equalized for example with the aid of quantum memory (see [107] for more details), some non-Gaussian states lead to enhanced *entanglement* transfer relative to that obtained by Gaussian state transfer.

The performance of CV-QKD protocols has been analysed in [109] for transmission over atmospheric fading channels, where the source is constituted by PSS states in the context of EB CV-QKD protocols. In [109], one mode of the PSS state remains at the ground station (satellite), while the other photon-subtracted mode is transmitted to the satellite (ground station) over the fading uplink (downlink) channel characterized by the probability distribution $p(\eta)$ and maximum transmission coefficient of η_0. When the transmission coefficient of the atmospheric channel can be measured in real time, after acquiring each realization of η, the key rate $K(\eta)$ is calculated based on the covariance matrix of the mixed non-Gaussian state at the output of the channel. The final key rate is then computed as $K = P_c \int_0^{\eta_0} K(\eta) p(\eta)\, d\eta$ in units of bits per pulse, with P_c being the creation probability of the initial non-Gaussian entangled state. The resultant key rate represents a lower bound on the actual key rate of the CV-QKD protocol. However, to determine the actual resultant key rates (not just its lower bounds), $K(\eta)$ must be computed based on the density operator of the mixed non-Gaussian output state.

In [107] and [109] the non-Gaussian operations are first applied to the initial Gaussian states, with the resultant non-Gaussian states being transmitted through the atmospheric fading channel. An alternative approach would be to transmit the initial Gaussian states through the atmospheric channel, and then apply the non-Gaussian operations after the atmospheric channel to the quantum states received. In [212], the distillation of CV entanglement using a coherent superposition-based non-Gaussian operation has been studied, where the non-Gaussian operation is the superposition of the photon subtraction and of the photon addition operations, and where the non-Gaussian operation is applied either before or after a fixed-attenuation channel.

VIII. Comparison With Discrete-Variable Technologies

The family of DV systems invoked for satellite-based quantum communications constitutes an alternative technology, which has been deployed in Micius [66]–[68]. In space-based deployment, a range of pragmatic issues comes into play when considering the pros and cons of DV *vs.* CV implementations. Perhaps the strongest argument in favour of DV systems in the space-based context is that photon losses have a less grave impact on quantum information processing in DV systems. In CV systems the photon losses in the channel introduce vacuum noise, leading to a reduction in the correlation between Alice and Bob's data. By contrast, in DV systems, photon losses reduce the communication efficiency, but they do not trigger a false single-photon detection event. A photon is either lost in the channel, in which case Bob does not register anything, or it is simply detected at Bob's detector. In high-loss scenarios, this effect can lead to advantages for DV systems. However, this benefit may by outweighed by other considerations, as discussed briefly below. More details on satellite-based DV quantum communication can be found elsewhere, for example in [40].

The performance of DV-QKD [231] is limited both by the difficulty of single-photon generation, as well as by the expense of single-photon detectors. It is a challenge to construct a true single-photon source owing to implementation challenges. Alternatively, single-photon sources can be approximated using an attenuated laser (weak coherent state pulses) [232], [233]. By contrast, CV-QKD systems rely on low-cost implementations and are potentially capable of supporting higher key rates than DV-QKD systems. Recall that CV-QKD can be implemented by modulating both the amplitude and phase quadratures of a coherent laser and can be subsequently measured in the receivers using homodyne detectors, which operate faster and more efficiently than the single-photon detectors. Moreover, CV-QKD systems are more compatible with standard telecommunication encoding, transmission and detection techniques. All these advantages potentially allow CV-QKD protocols to achieve higher secret key rates than DV-QKD systems.

Furthermore, the single-photon detectors of DV systems are very sensitive to background light sources. By contrast, the homodyne detectors used for CV systems offer beneficial robustness to background light. Indeed, an explicit advantage of using a local oscillator is that it has an 'automatic' spectral-domain filtering effect. Consequently, homodyne detectors remain to a large extent unimpaired in daylight conditions without the extra filtering that are needed by the single-photon detectors [16]. Furthermore, in CV systems, a tapped component of the local oscillator can be simply obtained and measured, thereby allowing for *direct* monitoring of atmospheric fluctuations effects, such as beam wandering (which can then be compensated for using adaptive optics [16], [98], [110]).

TABLE VI
Comparison of DV-QKD and CV-QKD

	DV-QKD	**CV-QKD**
Preparation	● Difficult to implement	● Low-cost implementation
Channel	● Photon losses do not trigger false detection events	●Photon losses introduce vacuum noise
Measurement	● Expensive ● Sensitive to background light	●Low-cost implementation ● Robust to background light ● Efficient (high key rates) ● Facilitates FSO channel estimation
Performance	● Generates higher key rates in high-loss channels	● Generates higher key rates in low-loss channels

Both DV and CV-QKD systems have protocols which are able to generate unconditional secure key [76]. However, the performance of QKD systems can be evaluated in terms of the generation "rate" of the final secure key. Due to the fact that the impact of photon losses on QKD performance is different for DV and CV systems (as discussed earlier), for low-loss channels where CV-QKD is secure (i.e., generates positive key rates), the key rate generated from CV-QKD can be higher than the key rate from DV-QKD [163] (due to the use of faster and more efficient transmission and detection technology in CV-QKD systems). However, for high-loss (and noisy) channels where CV-QKD is not secure (i.e., not able to generate positive key rates), DV-QKD can be secure, and generate positive key rates. Thus, the secure transmission range (or the maximum transmission distance) of DV-QKD systems can be higher than CV-QKD systems.

Table VI summarizes the pros and cons of DV-QKD and CV-QKD. Nonetheless, the issue of whether DV or CV systems should be deployed as the quantum information carrier in space-based quantum communications remains very much an open issue at the time of writing. Ultimately, it could well be that hybrid DV+CV architectures, accommodating time-variant atmospheric conditions, turn out to be the most beneficial in many circumstances. The employment of such hybrid architectures has been extensively studied for example in [234].

IX. Future Directions

Quantum communication via satellite is in its infancy. Building on the early work and verification studies (both experimental and theoretical) of many researchers, e.g., [16], [32]–[69], [78], [79], [93]–[112], [235], and [236] the pioneering experimental result of the Micius [66]–[68] collaboration has now provided us with the first glimpse of what is truly achievable via space-based platforms. However, there remains much to do before quantum communications via satellites can be considered mainstream. This is especially so in the CV quantum domain, where no space-based deployments have yet been achieved, despite the numerous theoretical studies, e.g., [16] and [98]–[111]. We briefly mention here some of the research topics within space-based CV quantum communications that we consider of particular interest to any multi-disciplinary engineering community.

A. Channel Transmissivity Measurements

The Micius [66]–[68] data provides us with our first real insight into the channel conditions experienced by quantum states, as they traverse through the turbulent atmosphere, to and from Earth. The measured photonic losses in the downlink [66], [67] and in the uplink [68] are now available (the losses in the latter case were a minimum of 41 dB). Leveraging this data for better understanding the channel conditions experienced by CV states as they travel to and from Earth would be an insightful, but costly endeavour. As discussed earlier in Section VIII, the loss of photons in the CV context fundamentally affects any subsequent information processing, as opposed to the DV case, where photons not received can be simply ignored. Ultimately, the study of how the CV states are affected by the atmosphere reduces to a determination of the statistical distribution of the channel transmissivity. Detailed knowledge of this distribution has wide ranging implications for studies pertaining to non-classical signatures of CV states traversing through atmospheric channels [104], as well as for a host of CV-based applications. The latter outcome is due to the fact that many applications are very sensitive to the channel's transmissivity [105]–[109]. As discussed previously, beyond the dominant effects of beam wandering and beam broadening, other more subtle effects induced by the atmosphere can play a non-negligible role. These effects include beam deformation, attenuation, absorption and scattering. Sophisticated theoretical studies of these effects are now becoming available, and in general these models are found to be consistent with terrestrial experiments carried out over a wide range of turbulence conditions [101], [237], [238]. Experimental confirmations of existing turbulence models in the realm of Earth-to-satellite (and vice versa) channels would be very important. Of particular importance would be a robust validation of the beam-wandering models used for the transmissivity statistics in the Earth-to satellite channels [100]–[102], and the validation of the beam-broadening models expected to dominate the satellite-to-Earth channels [57].

B. Error Reconciliation

The reconciliation phase of any QKD protocol is perhaps the area of quantum communications most closely associated with classical communications. In the DV scenario, long LDPC codes can be used to correct transmission errors. For scenarios, where DV quantum measurements are mapped directly to binary outcomes, the transmission of bits via a classical binary symmetric channel can be adopted as the underlying model. A range of high-performance LDPC codes which approach reconciliation factors close to 1 in the large key length limit are known for such channels [239]–[241]. However, in the CV setting the extraction of binary information is substantially more involved. Currently, there are two main techniques that are widely adopted in this regard, namely, slice reconciliation [20], [242], and multi-dimensional reconciliation [24], [243]. For the low signal to noise ratios (SNRs) routinely anticipated for satellite communications, the multi-dimensional reconciliation technique is likely to be more appropriate. In this context, multi-dimensional reconciliation via multi-edge LDPC codes is considered by many as the most appropriate path due to the high performance of such codes at low SNRs [24].

Nonetheless, numerous open research issues remain. Perhaps the most important of these is constituted by the finite key effects. Much of the work in formally determining the security of a key within QKD systems assumes having an infinite key length. However, in reality, this assumption is never satisfied and the consideration of the finite-length key effects must be analysed. This is an issue that affects both the DV [244] and CV security analyses [181], [245]–[248]. This problem is of particular concern for space-based QKD due to the short transit times of LEO satellites. Hence, the finite-length key processing invoked in the context of CV-QKD conceived for satellites has to be considered. Naturally, this analysis will be strongly dependent on the specific CV-QKD protocol adopted. Finite-length key based analyses of standard coherent state protocols [249], of MDI protocols [250], [251] and of full device-independent protocols [252] follow quite distinct paths.

Beyond the finite-length effects within the reconciliation decoding phase, the construction of near-capacity adaptive-rate LDPC codes for CV space-based implementations would be useful. Again, these issues are particularly relevant to satellite-based communication due to the time-variant properties of the channel. For LEO satellites we can expect the SNR to exhibit quite rapid variations versus time, as the satellite appears above the horizon and disappears again. Furthermore, for a given set of orbital parameters, we could anticipate the SNR's evolution versus time to be reasonably predictable. Adaptive-rate LDPC codes well suited for counteracting the SNR vs time evolution should be constructed. The employment of puncturing techniques [253] used for multi-edge LDPC codes appears to be an appropriate pathway to achieving this [254]. These studies are only in their early phases of development, hence further research into the design of adaptive-rate codes as a path to low-complexity CV-QKD via satellites is expected to be fruitful. An important focus of such future studies should be the maintenance of high reconciliation efficiencies over the anticipated range of SNRs [255].

Finally, we note that in principle other codes beyond LDPC codes could be used in the CV-QKD reconciliation phase. Currently, however, limited work has been reported in this area. Nonetheless, we do note some work on turbo codes [256] applied to the CV domain, as reported in [257] (for use of such codes in the DV domain see [258], [259]). Furthermore, polar codes [260] have recently been invoked for CV-QKD in [261]. These contributions suggest that further performance comparisons using various error correction codes for the CV-QKD reconciliation phase may become fruitful.

C. CV Quantum Error Correction Codes

Of special importance for CV quantum communications are the non-Gaussian operations that form the basis of quantum error correction. Such operations are required due to the no-go theorem, stipulating that Gaussian errors cannot be corrected by purely Gaussian operations [262]. It is possible to build a pathway from standard classical LDPC codes to qubit error correction codes, and then to CV error correction codes. Following on from the original CV error correction protocols of [263]–[265], there are several examples of CV quantum error correction codes appearing in [197] and [266]–[272]. However, in the context of space-based implementations there is evidence to suggest that direct non-Gaussian measurement at the receiver is likely to be the most fruitful pathway to CV error correction - at least in the short term.

In Section VII-A we have discussed a host of non-Gaussian operations in the form of photon subtraction and addition techniques that were used to form our non-Gaussian states, as seen in Fig. 23. Such operations can also be used for producing CV entanglement distillation - a form of quantum error correction for CV variables. Photon subtraction and addition techniques are becoming mainstream in laboratories throughout the world and the imminent integration of such techniques directly into future satellite communications is expected. In QKD implementations though, a balance must be struck between the relatively low probabilities of success for the subtraction/addition operations required and the resultant degradation of the key rates. More detailed studies of these design options for space-based communications are warranted.

D. The Interface With Classical Terrestrial Networks

Although fundamentally a breakthrough, the birth of space-based quantum communications can be seen from a more pragmatic perspective - it will allow for the creation of the global “Quantum Internet”. This new Internet will interconnect a vast range of devices, from mobile devices all the way through to the much anticipated quantum computers. These devices will be able to transfer quantum information and communicate with each other in an unconditionally secure manner. Importantly, this new network will consist of not only quantum communication channels but also of classical communication channels. As such, consideration of how best to accommodate integration of the quantum information received via satellites into a wider integrated network will be required. Currently, very little detailed thought has been given to this ambitious enterprise, and therefore there is much opportunity for high-impact future research in the context of the integrated system-oriented vision of Fig. 1.

In the CV setting, perhaps the integration of CV quantum information into the microwave setting is the most important example. The implementation of quantum communication protocols in the optical frequency domain is usually preferred, which is an explicit benefit of the negligible background thermal radiation at optical frequencies, hence all of our discussions have been in this domain. However, the advent of super-conducting microwave quantum circuits have led to an increasing interest in the implementation of quantum communication protocols in the microwave regime [129]–[131], [273]–[279]. These interests are further fuelled by advances in macro electro-optomechanical resonators that are capable of coupling quantum information with the microwave-optical interface [276], [278], [279]. With the advent of this technology, quantum information created via super-conducting circuits may be readily upconverted to the optical regime for direct transfer to an overhead satellite. The satellite could then communicate that information optically to a second terrestrial receiver with subsequent conversion back to the microwave regime for storage, error correction or further information processing. Such a scenario could well represent how future quantum computers will share information globally through the quantum Internet. We also note that it is even possible to directly transmit quantum information via microwave carriers to nearby wireless receivers [132]. The development of such integration techniques for the quantum Internet is still in its infancy.

X. Conclusion

We have discussed the recent research advances that are most relevant to CV quantum communication via low-Earth-orbit satellites. Recent experimental results gleaned from the Micius satellite on a range of DV-based quantum communication protocols indicate that CV quantum communication via large distances over the ether has become entirely plausible. We have outlined many of the technical advances in the field of CV quantum communication encompasses and highlighted a range of technical challenges it faces. As compared to the DV technology, CV systems bring with them the compelling benefit of inherent compatibility with the state-of-the-art optical technology. Explicitly, while DV sources and detectors are difficult to implement and expensive, CV systems can be easily implemented with the aid of off-the-shelf lasers and homodyne (or heterodyne) detectors. Hence, the many advantages of this intriguing technology warrant its experimental deployment to make the vision of the perfectly secure future quantum-communications scenario portrayed in Fig. 1 a reality.

Our hope is valued Colleague that you would join this community-effort...

References

[1] L. Hanzo *et al.*, “Wireless myths, realities, and futures: From 3G/4G to optical and quantum wireless,” *Proc. IEEE*, vol. 100, pp. 1853–1888, May 2012.

[2] P. Botsinis, S. X. Ng, and L. Hanzo, “Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design,” *IEEE Access*, vol. 1, pp. 94–122, 2013.

[3] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, Bengaluru, India, 1984, pp. 175–179.

[4] C. H. Bennett *et al.*, “Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels,” *Phys. Rev. Lett.*, vol. 70, no. 13, pp. 1895–1899, 1993.

[5] L. Vaidman, “Teleportation of quantum states,” *Phys. Rev. A*, vol. 49, no. 2, pp. 1473–1476, 1994.

[6] A. Furusawa *et al.*, “Unconditional quantum teleportation,” *Science*, vol. 282, no. 5389, pp. 706–709, 1998.

[7] P. van Loock and S. L. Braunstein, "Unconditional teleportation of continuous-variable entanglement," *Phys. Rev. A*, vol. 61, no. 1, 1999, Art. no. 010302.

[8] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[9] S. L. Braunstein and P. van Loock, "Quantum information with continuous variables," *Rev. Mod. Phys.*, vol. 77, no. 2, pp. 513–577, Jun. 2005.

[10] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992.

[11] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A*, vol. 61, Dec. 1999, Art. no. 010303(R).

[12] N. J. Cerf, M. Lévy, and G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states," *Phys. Rev. A*, vol. 63, no. 5, 2001, Art. no. 052311.

[13] F. Grosshans and P. Grangier, "Reverse reconciliation protocols for quantum cryptography with continuous variables," in *Proc. 6th Int. Conf. Quantum Commun. Meas. Comput.*, 2002.

[14] F. Grosshans *et al.*, "Quantum key distribution using Gaussian-modulated coherent states," *Nature*, vol. 421, pp. 238–241, Jan. 2003.

[15] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, "Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables," *Quantum Inf. Comput.*, vol. 3, no. 7, pp. 535–552, 2003.

[16] D. Elser *et al.*, "Feasibility of free space quantum key distribution with coherent polarization states," *New J. Phys.*, vol. 11, no. 4, 2009, Art. no. 045014.

[17] A. A. Semenov, F. Töppel, D. Y. Vasylyev, H. V. Gomonay, and W. Vogel, "Homodyne detection for atmosphere channels," *Phys. Rev. A*, vol. 85, no. 1, 2012, Art. no. 013826.

[18] C. Croal *et al.*, "Free-space quantum signatures using heterodyne measurements," *Phys. Rev. Lett.*, vol. 117, no. 10, 2016, Art. no. 100503.

[19] P. A. Hiskett *et al.*, "Long-distance quantum key distribution in optical fibre," *New J. Phys.*, vol. 8, Sep. 2006, Art. no. 193.

[20] J. Lodewyck *et al.*, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Phys. Rev. A*, vol. 76, no. 4, 2007, Art. no. 042305.

[21] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, "Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers," *Phys. Rev. A*, vol. 76, no. 5, 2007, Art. no. 052323.

[22] D. Rosenberg *et al.*, "Practical long-distance quantum key distribution system using decoy levels," *New J. Phys.*, vol. 11, Apr. 2009, Art. no. 045009.

[23] Q. D. Xuan, Z. Zhang, and P. L. Voss, "A 24 km fiber-based discretely signaled continuous variable quantum key distribution system," *Opt. Exp.*, vol. 17, no. 26, pp. 24244–24249, 2009.

[24] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nat. Photon.*, vol. 7, no. 5, pp. 378–381, 2013.

[25] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," *Sci. Rep.*, vol. 6, Jan. 2016, Art. no. 19201.

[26] H. Takesue *et al.*, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," *Nat. Photon.*, vol. 1, no. 6, pp. 343–348, 2007.

[27] D. Stucki *et al.*, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," *New J. Phys.*, vol. 11, no. 7, 2009, Art. no. 075003.

[28] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photon.*, vol. 8, pp. 595–604, Jul. 2014.

[29] B. Korzh *et al.*, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nat. Photon.*, vol. 9, no. 3, pp. 163–168, 2015.

[30] H.-L. Yin *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.*, vol. 117, no. 19, 2016, Art. no. 190501.

[31] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, pp. 5932–5935, Dec. 1998.

[32] C.-Z. Peng *et al.*, "Experimental free-space distribution of entangled photon pairs over 13 km: Towards satellite-based global quantum communication," *Phys. Rev. Lett.*, vol. 94, no. 15, 2005, Art. no. 150501.

[33] K. J. Resch *et al.*, "Distributing entanglement and single photons through an intra-city, free-space quantum channel," *Opt. Exp.*, vol. 13, no. 1, pp. 202–209, 2005.

[34] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, "Free-space quantum key distribution with entangled photons," *Appl. Phys. Lett.*, vol. 89, no. 10, 2006, Art. no. 101122.

[35] C. Erven, C. Couteau, R. Laflamme, and G. Weihs, "Entangled quantum key distribution over two free-space optical links," *Opt. Exp.*, vol. 16, no. 21, pp. 16840–16853, 2008.

[36] S. Nauerth *et al.*, "Air-to-ground quantum communication," *Nat. Photon.*, vol. 7, no. 5, pp. 382–386, 2013.

[37] J.-Y. Wang *et al.*, "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," *Nat. Photon.*, vol. 7, no. 5, pp. 387–393, 2013.

[38] J.-P. Bourgoin *et al.*, "Free-space quantum key distribution to a moving receiver," *Opt. Exp.*, vol. 23, no. 26, pp. 33437–33447, 2015.

[39] D. E. Bruschi, T. C. Ralph, I. Fuentes, T. Jennewein, and M. Razavi, "Spacetime effects on satellite-based quantum communications," *Phys. Rev. D*, vol. 90, no. 4, 2014, Art. no. 045041.

[40] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Inf.*, vol. 3, Aug. 2017, Art. no. 30.

[41] J. M. P. Armengol *et al.*, "Quantum communications at ESA: Towards a space experiment on the ISS," *Acta Astronautica*, vol. 63, nos. 1–4, pp. 165–178, 2008.

[42] T. Scheidl, E. Wille, and R. Ursin, "Quantum optics experiments using the international space station: A proposal," *New J. Phys.*, vol. 15, no. 4, 2013, Art. no. 043008.

[43] T. Jennewein *et al.*, "QEYSSAT: A mission proposal for a quantum receiver in space," in *Proc. SPIE*, vol. 8997. San Francisco, CA, USA, 2014, Art. no. 89970A.

[44] H. Xin, "Chinese academy takes space under its wing," *Science*, vol. 332, no. 6032, p. 904, 2011.

[45] R. Ursin *et al.*, "Space-quest, experiments with quantum entanglement in space," *Europhys. News*, vol. 40, no. 3, pp. 26–29, 2009.

[46] T. Jennewein and B. Higgins, "The quantum space race," *Phys. World*, vol. 26, no. 3, pp. 52–56, 2013.

[47] P. Villoresi *et al.*, "Experimental verification of the feasibility of a quantum channel between space and Earth," *New J. Phys.*, vol. 10, no. 3, 2008, Art. no. 033038.

[48] J. Yin *et al.*, "Experimental quasi-single-photon transmission from satellite to earth," *Opt. Exp.*, vol. 21, no. 17, pp. 20032–20040, 2013.

[49] G. Vallone *et al.*, "Experimental satellite quantum communications," *Phys. Rev. Lett.*, vol. 115, no. 4, 2015, Art. no. 040502.

[50] M. Er-Long *et al.*, "Background noise of satellite-to-ground quantum key distribution," *New J. Phys.*, vol. 7, no. 1, 2005, Art. no. 215.

[51] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New J. Phys.*, vol. 4, no. 1, 2002, Art. no. 82.

[52] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger, "Long-distance quantum communication with entangled photons using satellites," *IEEE J. Sel. Topics Quantum Electron.*, vol. 9, no. 6, pp. 1541–1551, Nov./Dec. 2003.

[53] C. Bonato *et al.*, "Influence of satellite motion on polarization qubits in a space-earth quantum communication link," *Opt. Exp.*, vol. 14, no. 21, pp. 10050–10059, 2006.

[54] C. Bonato, A. Tomaello, V. D. Deppo, G. Naletto, and P. Villoresi, "Feasibility of satellite quantum key distribution," *New J. Phys.*, vol. 11, Apr. 2009, Art. no. 045017.

[55] A. Tomaello, C. Bonato, V. Da Deppo, G. Naletto, and P. Villoresi, "Link budget and background noise for satellite quantum key distribution," *Adv. Space Res.*, vol. 47, no. 5, pp. 802–810, 2011.

[56] E. Meyer-Scott *et al.*, "How to implement decoy-state quantum key distribution for a satellite uplink with 50-db channel loss," *Phys. Rev. A*, vol. 84, Dec. 2011, Art. no. 062326.

[57] J.-P. Bourgoin *et al.*, "A comprehensive design and performance analysis of low earth orbit satellite quantum communication," *New J. Phys.*, vol. 15, no. 2, 2013, Art. no. 023006.

[58] L. Moli-Sanchez, A. Rodriguez-Alonso, and G. Seco-Granados, "Performance analysis of quantum cryptography protocols in optical earth-satellite and intersatellite links," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 9, pp. 1582–1590, Dec. 2009.

[59] Z. Yan *et al.*, "Novel high-speed polarization source for decoy-state BB84 quantum key distribution over free space and satellite links," *J. Lightw. Technol.*, vol. 31, no. 9, pp. 1399–1408, May 1, 2013.

[60] C. Cheng, R. Chandrasekara, Y. C. Tan, and A. Ling, "Space-qualified nanosatellite electronics platform for photon pair experiments," *J. Lightw. Technol.*, vol. 33, no. 23, pp. 4799–4804, Dec. 1, 2015.

[61] B. Qi *et al.*, "A compact readout electronics for the ground station of a quantum communication satellite," *IEEE Trans. Nucl. Sci.*, vol. 62, no. 3, pp. 883–888, Jun. 2015.

[62] L. Bacsardi, "On the way to quantum-based satellite communication," *IEEE Commun. Mag.*, vol. 51, no. 8, pp. 50–55, Aug. 2013.

[63] L. Bacsardi, "Satellite communication over quantum channel," *Acta Astronautica*, vol. 61, nos. 1–6, pp. 151–159, 2007.

[64] Z. Tang *et al.*, "Generation and analysis of correlated pairs of photons aboard a nanosatellite," *Phys. Rev. Appl.*, vol. 5, no. 5, 2016, Art. no. 054022.

[65] H. Takenaka *et al.*, "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite," *Nat. Photon.*, vol. 11, no. 8, pp. 502–508, 2017.

[66] S.-K. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[67] J. Yin *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[68] J.-G. Ren *et al.*, "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, pp. 70–73, Sep. 2017.

[69] K. Boone *et al.*, "Entanglement over global distances via quantum repeaters with satellite links," *Phys. Rev. A*, vol. 91, no. 5, 2015, Art. no. 052325.

[70] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[71] G. S. Vernam, "Cipher printing telegraph systems: For secret wire and radio telegraphic communications," *J. Amer. Inst. Elect. Eng.*, vol. 45, pp. 109–115, Jan. 1926.

[72] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, Oct. 1982.

[73] D. Dieks, "Communication by EPR devices," *Phy. Lett. A*, vol. 92, no. 6, pp. 271–272, 1982.

[74] R. Renner, "Security of quantum key distribution," Ph.D. dissertation, ETH Zurich, Zürich, Switzerland, 2005.

[75] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols," *Phys. Rev. A*, vol. 72, no. 1, 2005, Art. no. 012332.

[76] V. Scarani *et al.*, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep. 2009.

[77] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

[78] R. Ursin *et al.*, "Entanglement-based quantum communication over 144km," *Nat. Phys.*, vol. 3, no. 7, pp. 481–486, 2007.

[79] T. Schmitt-Manderbach *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, no. 1, 2007, Art. no. 010504.

[80] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, "Continuous variable quantum key distribution with modulated entangled states," *Nat. Commun.*, vol. 3, Sep. 2012, Art. no. 1083.

[81] S. Pirandola and S. Mancini, "Quantum teleportation with continuous variables: A survey," *Laser Phys.*, vol. 16, no. 10, pp. 1418–1438, 2006.

[82] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, "Advances in quantum teleportation," *Nat. Photon.*, vol. 9, pp. 641–652, Sep. 2015.

[83] G. Adesso and F. Illuminati, "Entanglement in continuous-variable systems: Recent advances and current perspectives," *J. Phys. A Math. Theor.*, vol. 40, no. 28, pp. 7821–7880, 2007.

[84] N. Gisin and R. Thew, "Quantum communication," *Nat. Photon.*, vol. 1, pp. 165–171, Mar. 2007.

[85] U. L. Andersen, G. Leuchs, and C. Silberhorn, "Continuous-variable quantum information processing," *Laser Photon. Rev.*, vol. 4, pp. 337–354, Apr. 2010.

[86] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, "Quantum information with Gaussian states," *Phys. Rep.*, vol. 448, nos. 1–4, pp. 1–111, 2007.

[87] C. Weedbrook *et al.*, "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, pp. 621–669, May 2012.

[88] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photon.*, vol. 8, pp. 595–604, Jul. 2014.

[89] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Inf.*, vol. 2, Nov. 2016, Art. no. 16025.

[90] M. Peev *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, Jul. 2009, Art. no. 075001.

[91] M. Sasaki *et al.*, "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Exp.*, vol. 19, no. 11, pp. 10387–10409, 2011.

[92] B. Fröhlich *et al.*, "A quantum access network," *Nature*, vol. 501, pp. 69–72, Sep. 2013.

[93] T. Scheidl *et al.*, "Feasibility of 300 km quantum key distribution with entangled states," *New J. Phys.*, vol. 11, Aug. 2009, Art. no. 085002.

[94] A. Fedrizzi *et al.*, "High-fidelity transmission of entanglement over a high-loss free-space channel," *Nat. Phys.*, vol. 5, no. 6, pp. 389–392, 2009.

[95] J. Yin *et al.*, "Quantum teleportation and entanglement distribution over 100-kilometre free-space channels," *Nature*, vol. 488, pp. 185–188, Aug. 2012.

[96] X.-S. Ma *et al.*, "Quantum teleportation over 143 kilometres using active feedforward," *Nature*, vol. 489, no. 7415, pp. 269–273, 2012.

[97] S.-K. Liao *et al.*, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nat. Photon.*, vol. 11, no. 8, pp. 509–513, 2017.

[98] B. Heim *et al.*, "Atmospheric channel characteristics for quantum communication with continuous polarization variables," *Appl. Phys. B*, vol. 98, no. 4, pp. 635–640, 2010.

[99] A. A. Semenov and W. Vogel, "Quantum light in the turbulent atmosphere," *Phys. Rev. A*, vol. 80, no. 2, 2009, Art. no. 021802(R).

[100] D. Y. Vasylyev, A. A. Semenov, and W. Vogel, "Toward global quantum communication: Beam wandering preserves nonclassicality," *Phys. Rev. Lett.*, vol. 108, Jun. 2012, Art. no. 220501.

[101] D. Vasylyev, A. A. Semenov, and W. Vogel, "Atmospheric quantum channels with weak and strong turbulence," *Phys. Rev. Lett.*, vol. 117, Aug. 2016, Art. no. 090501.

[102] V. C. Usenko *et al.*, "Entanglement of Gaussian states and the applicability to quantum key distribution over fading channels," *New J. Phys.*, vol. 14, Sep. 2012, Art. no. 093048.

[103] M. Bohmann, A. A. Semenov, J. Sperling, and W. Vogel, "Gaussian entanglement in the turbulent atmosphere," *Phys. Rev. A*, vol. 94, Jul. 2016, Art. no. 010302(R).

[104] M. Bohmann, J. Sperling, A. A. Semenov, and W. Vogel, "Higher-order nonclassical effects in fluctuating-loss channels," *Phys. Rev. A*, vol. 95, Jan. 2017, Art. no. 012324.

[105] N. Hosseinidehaj and R. Malaney, "Gaussian entanglement distribution via satellite," *Phys. Rev. A*, vol. 91, Feb. 2015, Art. no. 022304.

[106] N. Hosseinidehaj and R. Malaney, "Quantum key distribution over combined atmospheric fading channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., 2015, pp. 7413–7419.

[107] N. Hosseinidehaj and R. Malaney, "Entanglement generation via non-Gaussian transfer over atmospheric fading channels," *Phys. Rev. A*, vol. 92, Dec. 2015, Art. no. 062336.

[108] N. Hosseinidehaj and R. Malaney, "CV-MDI quantum key distribution via satellite," *Quantum Inf. Comput.*, vol. 17, nos. 5–6, pp. 361–379, 2017.

[109] N. Hosseinidehaj and R. Malaney, "CV-QKD with Gaussian and non-Gaussian entangled states over satellite-based channels," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Washington, DC, USA, 2016, pp. 1–7.

[110] B. Heim *et al.*, "Atmospheric continuous-variable quantum communication," *New J. Phys.*, vol. 16, Nov. 2014, Art. no. 113018.

[111] C. Peuntinger *et al.*, "Distribution of squeezed states through an atmospheric channel," *Phys. Rev. Lett.*, vol. 113, Aug. 2014, Art. no. 060502.

[112] K. Günthner *et al.*, "Quantum-limited measurements of optical signals from a geostationary satellite," *Optica*, vol. 4, no. 6, pp. 611–616, 2017.

[113] J. Eisert and M. B. Plenio, "Introduction to the basics of entanglement theory in continuous-variable systems," *Int. J. Quantum Inf.*, vol. 1, pp. 479–506, Nov. 2003.

[114] G. Adesso, "Entanglement of Gaussian states," Ph.D. dissertation, Dept. Phys., Univ. Salerno, Fisciano, Italy, 2007.

[115] C. C. Gerry and P. L. Knight, *Introductory Quantum Optics*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[116] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, Jan. 2002, Art. no. 057902.

[117] C. Weedbrook *et al.*, "Quantum cryptography without switching," *Phys. Rev. Lett.*, vol. 93, Oct. 2004, Art. no. 170504.

[118] R. García-Patrón and N. J. Cerf, "Continuous-variable quantum key distribution protocols over noisy channels," *Phys. Rev. Lett.*, vol. 102, Mar. 2009, Art. no. 130501.

[119] J. G. Rarity, P. R. Tapster, and E. Jakeman, "Observation of sub-poissonian light in parametric downconversion," *Opt. Commun.*, vol. 62, no. 3, pp. 201–206, 1987.

[120] P. G. Kwiat *et al.*, "New high-intensity source of polarization-entangled photon pairs," *Phys. Rev. Lett.*, vol. 75, pp. 4337–4341, Dec. 1995.

[121] M. E. Anderson, D. F. McAlister, M. G. Raymer, and M. C. Gupta, "Pulsed squeezed-light generation in $\chi^{(2)}$ nonlinear waveguides," *J. Opt. Soc. Amer. B*, vol. 14, no. 11, pp. 3180–3190, 1997.

[122] W. P. Grice and I. A. Walmsley, "Spectral information and distinguishability in type-II down-conversion with a broadband pump," *Phys. Rev. A*, vol. 56, pp. 1627–1634, Aug. 1997.

[123] Y. Shih, "Entangled biphoton source—Property and preparation," *Rep. Progr. Phys.*, vol. 66, no. 6, pp. 1009–1044, 2003.

[124] R. Simon, "Peres–Horodecki separability criterion for continuous variable systems," *Phys. Rev. Lett.*, vol. 84, pp. 2726–2729, Mar. 2000.

[125] G. Giedke, M. M. Wolf, O. Krüger, R. F. Werner, and J. I. Cirac, "Entanglement of formation for symmetric Gaussian states," *Phys. Rev. Lett.*, vol. 91, Sep. 2003, Art. no. 107901.

[126] M. M. Wolf, G. Giedke, O. Krüger, R. F. Werner, and J. I. Cirac, "Gaussian entanglement of formation," *Phys. Rev. A*, vol. 69, May 2004, Art. no. 052320.

[127] G. Vidal and R. F. Werner, "Computable measure of entanglement," *Phys. Rev. A*, vol. 65, Feb. 2002, Art. no. 032314.

[128] M. B. Plenio, "Logarithmic negativity: A full entanglement monotone that is not convex," *Phys. Rev. Lett.*, vol. 95, Sep. 2005, Art. no. 090503.

[129] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, "Quantum cryptography approaching the classical limit," *Phys. Rev. Lett.*, vol. 105, Sep. 2010, Art. no. 110501.

[130] C. Weedbrook, S. Pirandola, and T. C. Ralph, "Continuous-variable quantum key distribution using thermal states," *Phys. Rev. A*, vol. 86, Aug. 2012, Art. no. 022318.

[131] C. Weedbrook, C. Ottaviani, and S. Pirandola, "Two-way quantum cryptography at different wavelengths," *Phys. Rev. A*, vol. 89, Jan. 2014, Art. no. 012309.

[132] N. Hosseinidehaj and R. Malaney, "Quantum entanglement distribution in next-generation wireless communication systems," in *Proc. 85th IEEE Veh. Technol. Conf. (VTC)*, 2017, pp. 1–7.

[133] N. Hosseinidehaj and R. Malaney, "Multimode entangled states in the lossy channel," in *Proc. IEEE VTC Int. Workshop Quantum Commun. Future Netw. (QCFN)*, Sydney, NSW, Australia, 2017, pp. 1–5.

[134] S. Pirandola, "Entanglement reactivation in separable environments," *New J. Phys.*, vol. 15, Nov. 2013, Art. no. 113046.

[135] R. Garcia-Patron, "Quantum information with optical continuous variables: From bell tests to key distribution," Ph.D. dissertation, Center Quant. Inf. Commun., Universite Libre de Bruxelles, Brussels, Belgium, 2007.

[136] C. Weedbrook, "Continuous-variable quantum key distribution with entanglement in the middle," *Phys. Rev. A*, vol. 87, Feb. 2013, Art. no. 022308.

[137] T. Symul *et al.*, "Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise," *Phys. Rev. A*, vol. 76, Sep. 2007, Art. no. 030303.

[138] S. Fossier *et al.*, "Field test of a continuous-variable quantum key distribution prototype," *New J. Phys.*, vol. 11, no. 13, 2009, Art. no. 045023.

[139] Y. Shen, H. Zou, L. Tian, P. Chen, and J. Yuan, "Experimental study on discretely modulated continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 82, Aug. 2010, Art. no. 022317.

[140] P. Jouguet *et al.*, "Field test of classical symmetric encryption with continuous variables quantum key distribution," *Opt. Exp.*, vol. 20, no. 13, pp. 14030–14041, 2012.

[141] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, "Direct and reverse secret-key capacities of a quantum channel," *Phys. Rev. Lett.*, vol. 102, Feb. 2009, Art. no. 050503.

[142] R. Renner and J. I. Cirac, "De Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," *Phys. Rev. Lett.*, vol. 102, no. 11, 2009, Art. no. 110504.

[143] R. García-Patrón and N. J. Cerf, "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution," *Phys. Rev. Lett.*, vol. 97, no. 6, 2006, Art. no. 190503.

[144] L. C. Andrews, R. L. Phillips, and C. Y. Hopen, *Laser Beam Scintillation With Applications*. Bellingham, WA, USA: SPIE, 2001.

[145] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Media*, vol. PM152, 2nd ed. Bellingham, WA, USA: SPIE, 2005.

[146] F. Dios, J. A. Rubio, A. Rodrfguez, and A. Comerón, "Scintillation and beam-wander analysis in an optical ground station-satellite uplink," *Appl. Opt.*, vol. 43, no. 19, pp. 3866–3873, 2004.

[147] H. Kaushal and G. Kaddoum, "Optical communication in space: Challenges and mitigation techniques," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 57–96, 1st Quart., 2017.

[148] K. S. Shaik, "Atmospheric propagation effects relevant to optical communications," TDA Progr., Lijnden, The Netherlands, Rep. 42-94, pp. 180–200, 1988.

[149] I. Capraro *et al.*, "Impact of turbulence in long range quantum and classical communications," *Phys. Rev. Lett.*, vol. 109, Nov. 2012, Art. no. 200502.

[150] G. Vallone *et al.*, "Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels," *Phys. Rev. A*, vol. 91, Apr. 2015, Art. no. 042320.

[151] X. Yi and M. Yao, "Free-space communications over exponentiated Weibull turbulence channels with nonzero boresight pointing errors," *Opt. Exp.*, vol. 23, no. 3, pp. 2904–2917, 2015.

[152] M. A. Esmail, H. Fathallah, and M.-S. Alouini, "Analysis of fog effects on terrestrial free space optical communication links," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, 2016, pp. 151–156.

[153] H. Kaushal, V. K. Jain, and S. Kar, *Free Space Optical Communication*, 1st ed. New Delhi, India: Springer, 2017.

[154] I. I. Kim, B. McArthur, and E. J. Korevaar, "Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications," in *Proc. Opt. Wireless Commun. III*, vol. 4214, 2001, pp. 26–38.

[155] P. W. Kruse, L. D. McGlauchlin, and R. B. McQuistan, *Elements of Infrared Technology: Generation, Transmission and Detection*. New York, NY, USA: Wiley, 1962.

[156] J. B. Pors, "Entangling light in high dimensions," Ph.D. dissertation, Casimir Res. School, Leiden Univ., Leiden, The Netherlands, 2011.

[157] P. W. Milonni, J. H. Carter, C. G. Peterson, and R. J. Hughes, "Effects of propagation through atmospheric turbulence on photon statistics," *J. Opt. B Quantum Semiclassical Opt.*, vol. 6, no. 6, pp. S742–S745, 2004.

[158] C. Erven *et al.*, "Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere," *New J. Phys.*, vol. 14, Dec. 2012, Art. no. 123018.

[159] H.-R. Li, F.-L. Li, Y. Yang, and Q. Zhang, "Entanglement swapping of two-mode Gaussian states in a thermal environment," *Phys. Rev. A*, vol. 71, Feb. 2005, Art. no. 022314.

[160] S. Pirandola, D. Vitali, P. Tombesi, and S. Lloyd, "Macroscopic entanglement by entanglement swapping," *Phys. Rev. Lett.*, vol. 97, Oct. 2006, Art. no. 150403.

[161] M. Abdi, S. Pirandola, P. Tombesi, and D. Vitali, "Continuous-variable-entanglement swapping and its local certification: Entangling distant mechanical modes," *Phys. Rev. A*, vol. 89, no. 2, 2014, Art. no. 022331.

[162] J. Hoelscher-Obermaier and P. van Loock, "Optimal Gaussian entanglement swapping," *Phys. Rev. A*, vol. 83, Jan. 2011, Art. no. 012319.

[163] S. Pirandola *et al.*, "High-rate measurement-device-independent quantum cryptography," *Nat. Photon.*, vol. 9, pp. 397–402, May 2015.

[164] S. L. Braunstein, and S. Pirandola, "Side-channel-free quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, 2012, Art. no. 130502.

[165] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, Mar. 2012, Art. no. 130503.

[166] T. Eberle, V. Händchen, and R. Schnabel, "Stable control of 10 dB two-mode squeezed vacuum states of light," *Opt. Exp.*, vol. 21, no. 9, pp. 11546–11553, 2013.

[167] H. Vahlbruch, M. Mehmet, K. Danzmann, and R. Schnabel, "Detection of 15 dB squeezed states of light and their application for the absolute calibration of photoelectric quantum efficiency," *Phys. Rev. Lett.*, vol. 117, Sep. 2016, Art. no. 110801.

[168] X.-C. Ma, S.-H. Sun, M.-S. Jiang, M. Gui, and L.-M. Liang, "Gaussian-modulated coherent-state measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 89, Apr. 2014, Art. no. 042335.

[169] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, "Continuous-variable measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 89, May 2014, Art. no. 052301.

[170] Y.-C. Zhang *et al.*, "Continuous-variable measurement-device-independent quantum key distribution using squeezed states," *Phys. Rev. A*, vol. 90, Nov. 2014, Art. no. 052325.

[171] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, "Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric configuration," *Phys. Rev. A*, vol. 91, Feb. 2015, Art. no. 022320.

[172] Y. Zhang *et al.*, "Noiseless linear amplifiers in entanglement-based continuous-variable quantum key distribution," *Entropy*, vol. 17, no. 7, pp. 4547–4562, 2015.

[173] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, "Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks," *Phys. Rev. Lett.*, vol. 111, Sep. 2013, Art. no. 130501.

[174] T. F. da Silva *et al.*, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits," *Phys. Rev. A*, vol. 88, Nov. 2013, Art. no. 052303.

[175] Y. Liu *et al.*, "Experimental measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 111, Sep. 2013, Art. no. 130502.

[176] Y.-L. Tang *et al.*, "Measurement-device-independent quantum key distribution over 200 km," *Phys. Rev. Lett.*, vol. 113, Nov. 2014, Art. no. 190501.

[177] Y.-L. Tang *et al.*, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Phys. Rev. X*, vol. 6, Mar. 2016, Art. no. 011024.

[178] M. Tomamichel and R. Renner, "Uncertainty relation for smooth entropies," *Phys. Rev. Lett.*, vol. 106, Mar. 2011, Art. no. 110506.

[179] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, "One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering," *Phys. Rev. A*, vol. 85, Jan. 2012, Art. no. 010301(R).

[180] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner, "A monogamy-of-entanglement game with applications to device-independent quantum cryptography," *New J. Phys.*, vol. 15, Oct. 2013, Art. no. 103002.

[181] T. Gehring *et al.*, "Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks," *Nat. Commun.*, vol. 6, Oct. 2015, Art. no. 8795.

[182] N. Walk *et al.*, "Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution," *Optica*, vol. 3, no. 6, pp. 634–642, 2016.

[183] K. Marshall and C. Weedbrook, "Device-independent quantum cryptography for continuous variables," *Phys. Rev. A*, vol. 90, no. 4, 2014, Art. no. 042311.

[184] R. Dong *et al.*, "Continuous-variable entanglement distillation of non-Gaussian mixed states," *Phys. Rev. A*, vol. 82, Jul. 2010, Art. no. 012312.

[185] P. Papanastasiou, C. Weedbrook, and S. Pirandola, "Continuous-variable quantum key distribution in uniform fast-fading channels," *Phys. Rev. A*, vol. 97, no. 3, Mar. 2018, Art. no. 032311. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.97.032311, doi: 10.1103/PhysRevA.97.032311.

[186] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nat. Commun.*, vol. 8, Apr. 2017, Art. no. 15043.

[187] C. H. Bennett *et al.*, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Phys. Rev. Lett.*, vol. 76, pp. 722–725, Jan. 1996.

[188] D. E. Browne, J. Eisert, S. Scheel, and M. B. Plenio, "Driving non-Gaussian to Gaussian states with linear optics," *Phys. Rev. A*, vol. 67, Jun. 2003, Art. no. 062320.

[189] J. Eisert, D. E. Browne, S. Scheel, and M. B. Plenio, "Distillation of continuous-variable entanglement with optical means," *Ann. Phys.*, vol. 311, no. 2, pp. 431–458, 2004.

[190] J. Fiurášek, P. Marek, R. Filip, and R. Schnabel, "Experimentally feasible purification of continuous-variable entanglement," *Phys. Rev. A*, vol. 75, no. 5, 2007, Art. no. 050302(R).

[191] A. P. Lund and T. C. Ralph, "Continuous-variable entanglement distillation over a general lossy channel," *Phys. Rev. A*, vol. 80, Sep. 2009, Art. no. 032309.

[192] J. Eisert, S. Scheel, and M. B. Plenio, "Distilling Gaussian states with Gaussian operations is impossible," *Phys. Rev. Lett.*, vol. 89, no. 13, 2002, Art. no. 137903.

[193] G. Giedke and J. I. Cirac, "Characterization of Gaussian operations and distillation of Gaussian states," *Phys. Rev. A*, vol. 66, Sep. 2002, Art. no. 032316.

[194] J. Fiurášek, "Gaussian transformations and distillation of entangled Gaussian states," *Phys. Rev. Lett.*, vol. 89, no. 13, 2002, Art. no. 137904.

[195] T. C. Ralph and A. P. Lund, "Nondeterministic noiseless linear amplification of quantum systems," in *Proc. 9th Int. Conf. Quantum Commun. Meas. Comput. (QCMC)*, 2009, pp. 155–160.

[196] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, "Heralded noiseless linear amplification and distillation of entanglement," *Nat. Photon.*, vol. 4, no. 5, pp. 316–319, 2010.

[197] T. C. Ralph, "Quantum error correction of continuous-variable states against Gaussian noise," *Phys. Rev. A*, vol. 84, Aug. 2011, Art. no. 022339.

[198] N. Walk, A. P. Lund, and T. C. Ralph, "Nondeterministic noiseless amplification via non-symplectic phase space transformations," *New J. Phys.*, vol. 15, Jul. 2013, Art. no. 073014.

[199] H. M. Chrzanowski *et al.*, "Measurement-based noiseless linear amplification for quantum communication," *Nat. Photon.*, vol. 8, pp. 333–338, Mar. 2014.

[200] A. E. Ulanov *et al.*, "Undoing the effect of loss on quantum entanglement," *Nat. Photon.*, vol. 9, Oct. pp. 764–768, 2015.

[201] J. Fiurášek and N. J. Cerf, "Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 86, no. 6, 2012, Art. no. 060302.

[202] R. Blandino *et al.*, "Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier," *Phys. Rev. A*, vol. 86, Jul. 2012, Art. no. 012327.

[203] N. Walk, T. C. Ralph, T. Symul, and P. K. Lam, "Security of continuous-variable quantum cryptography with Gaussian postselection," *Phys. Rev. A*, vol. 87, Feb. 2013, Art. no. 020303.

[204] T. Opatrný, G. Kurizki, and D.-G. Welsch, "Improvement on teleportation of continuous variables by photon subtraction via conditional measurement," *Phys. Rev. A*, vol. 61, Feb. 2000, Art. no. 032302.

[205] A. Kitagawa, M. Takeoka, M. Sasaki, and A. Chefles, "Entanglement evaluation of non-Gaussian states generated by photon subtraction from squeezed states," *Phys. Rev. A*, vol. 73, no. 2, Apr. 2006, Art. no. 042310.

[206] F. Dell'Anno, S. De Siena, L. Albano, and F. Illuminati, "Continuous-variable quantum teleportation with non-Gaussian resources," *Phys. Rev. A*, vol. 76, 2007, Art. no. 022301.

[207] Y. Yang and F.-L. Li, "Entanglement properties of non-Gaussian resources generated via photon subtraction and addition and continuous-variable quantum-teleportation improvement," *Phys. Rev. A*, vol. 80, no. 2, 2009, Art. no. 022315.

[208] S. L. Zhang and P. van Loock, "Distillation of mixed-state continuous-variable entanglement by photon subtraction," *Phys. Rev. A*, vol. 82, Dec. 2010, Art. no. 062316.

[209] C. Navarrete-Benlloch, R. Garcia-Patrón, J. H. Shapiro, and N. J. Cerf, "Enhancing quantum entanglement by photon addition and subtraction," *Phys. Rev. A*, vol. 86, Jul. 2012, Art. no. 012328.

[210] T. J. Bartley *et al.*, "Strategies for enhancing quantum entanglement by local photon subtraction," *Phys. Rev. A*, vol. 87, Feb. 2013, Art. no. 022313.

[211] S. L. Zhang, Y. Dong, X. Zou, B. Shi, and G. C. Guo, "Continuous-variable-entanglement distillation with photon addition," *Phys. Rev. A*, vol. 88, Sep. 2013, Art. no. 032324.

[212] J. Lee and H. Nha, "Entanglement distillation for continuous variables in a thermal environment: Effectiveness of a non-Gaussian operation," *Phys. Rev. A*, vol. 87, Mar. 2013, Art. no. 032307.

[213] K. P. Seshadreesan, J. P. Dowling, and G. S. Agarwal, "Non-Gaussian entangled states and quantum teleportation of Schrodinger-cat states," *Physica Scripta*, vol. 90, no. 7, 2015, Art. no. 074029.

[214] T. J. Bartley and I. A. Walmsley, "Directly comparing entanglement-enhancing non-Gaussian operations," *New J. Phys.*, vol. 17, Feb. 2015, Art. no. 023038.

[215] M. Allegra, P. Giorda, and M. G. A. Paris, "Role of initial entanglement and non-Gaussianity in the decoherence of photon-number entangled states evolving in a noisy channel," *Phys. Rev. Lett.*, vol. 105, Sep. 2010, Art. no. 100503.

[216] G. Adesso, "Simple proof of the robustness of Gaussian entanglement in bosonic noisy channels," *Phys. Rev. A*, vol. 83, Feb. 2011, Art. no. 024301.

[217] K. K. Sabapathy, J. S. Ivan, and R. Simon, "Robustness of non-Gaussian entanglement against noisy amplifier and attenuator environments," *Phys. Rev. Lett.*, vol. 107, no. 13, 2011, Art. no. 130501.

[218] S. N. Filippov and M. Ziman, "Entanglement sensitivity to signal attenuation and amplification," *Phys. Rev. A*, vol. 90, Jul. 2014, Art. no. 010301(R).

[219] P. Huang, G. He, J. Fang, and G. Zeng, "Performance improvement of continuous-variable quantum key distribution via photon subtraction," *Phys. Rev. A*, vol. 87, Jan. 2013, Art. no. 012317.

[220] Z. Li *et al.*, "Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 93, Jan. 2016, Art. no. 012310.

[221] L. F. M. Borelli, L. S. Aguiar, J. A. Roversi, and A. Vidiella-Barranco, "Quantum key distribution using continuous-variable non-Gaussian states," *Quantum Inf. Process.*, vol. 15, no. 2, pp. 893–904, 2016.

[222] G. S. Agarwal, S. Chaturvedi, and A. Rai, "Amplification of maximally-path-entangled number states," *Phys. Rev. A*, vol. 81, Apr. 2010, Art. no. 043843.

[223] H. Nha, G. J. Milburn, and H. J. Carmichael, "Linear amplification and quantum cloning for non-Gaussian continuous variables," *New J. Phys.*, vol. 12, Oct. 2010, Art. no. 103010.

[224] A. Leverrier and P. Grangier, "Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation," *Phy. Rev. A*, vol. 83, Apr. 2011, Art. no. 042312.

[225] K. Wakui, H. Takahashi, A. Furusawa, and M. Sasaki, "Photon subtracted squeezed states generated with periodically poled $KTiOPO_4$," *Opt. Exp.*, vol. 15, no. 6, pp. 3568–3574, 2007.

[226] H. Takahashi *et al.*, "Entanglement distillation from Gaussian input states," *Nat. Photon.*, vol. 4, pp. 178–181, Feb. 2010.

[227] Y. Kurochkin, A. S. Prasad, and A. I. Lvovsky, "Distillation of the two-mode squeezed state," *Phys. Rev. Lett.*, vol. 112, no. 7, 2014, Art. no. 070402.

[228] A. Zavatta, S. Viciani, and M. Bellini, "Quantum-to-classical transition with single-photon-added coherent states of light," *Science*, vol. 306, no. 5696, pp. 660–662, 2004.

[229] A. Zavatta, V. Parigi, and M. Bellini, "Experimental nonclassicality of single-photon-added thermal light states," *Phys. Rev. A*, vol. 75, May 2007, Art. no. 052106.

[230] J. S. Ivan, K. K. Sabapathy, and R. Simon, "Operator-sum representation for bosonic Gaussian channels," *Phys. Rev. A*, vol. 84, Oct. 2011, Art. no. 042311.

[231] H. V. Nguyen *et al.*, "Network coding aided cooperative quantum key distribution over free-space optical channels," *IEEE Access*, vol. 5, pp. 12301–12317, 2017.

[232] H. Weier, T. Schmitt-Manderbach, N. Regner, C. Kurtsiefer, and H. Weinfurter, "Free space quantum key distribution: Towards a real life application," *Fortschritte der Physik*, vol. 54, nos. 8–10, pp. 840–845, 2006.

[233] M. Jofre *et al.*, "Fast optical source for quantum key distribution based on semiconductor optical amplifiers," *Opt. Exp.*, vol. 19, no. 5, pp. 3825–3834, 2011.

[234] U. L. Andersen, J. S. Neergaard-Nielsen, P. van Loock, and A. Furusawa, "Hybrid discrete- and continuous-variable quantum information," *Nat. Phys.*, vol. 11, pp. 713–719, Sep. 2015.

[235] M. O. Gumberidze, A. A. Semenov, D. Vasylyev, and W. Vogel, "Bell nonlocality in the turbulent atmosphere," *Phys. Rev. A*, vol. 94, Nov. 2016, Art. no. 053801.

[236] A. A. Semenov and W. Vogel, "Entanglement transfer through the turbulent atmosphere," *Phys. Rev. A*, vol. 81, Feb. 2010, Art. no. 023835.

[237] O. O. Chumak and R. A. Baskov, "Strong enhancing effect of correlations of photon trajectories on laser beam scintillations," *Phys. Rev. A*, vol. 93, Mar. 2016, Art. no. 033821.

[238] M. Bohmann, R. Kruse, J. Sperling, C. Silberhorn, and W. Vogel, "Probing free-space quantum channels with laboratory-based experiments," *Phys. Rev. A*, vol. 95, Jun. 2017, Art. no. 063801.

[239] D. Elkouss, A. Leverrier, R. Alleaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seoul, South Korea, 2009, pp. 1879–1883.

[240] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, "Key reconciliation with low-density parity-check codes for long-distance quantum cryptography," *arXiv:1702.07740*, 2017.

[241] X. Wang, Y. Zhang, S. Yu, and H. Guo, "High speed information reconciliation for long distance continuous-variable quantum key distribution system," in *Front. Opt. OSA Tech. Dig. Opt. Soc. America*, p. JW4A.36.

[242] M. Bloch, A. Thangaraj, and S. W. McLaughlin, "Efficient reconciliation of correlated continuous random variables using LDPC codes," *arXiv:cs/0509041*, 2005.

[243] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 77, Apr. 2008, Art. no. 042325.

[244] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nat. Commun.*, vol. 3, Jan. 2012, Art. no. 634.

[245] A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 81, Jun. 2010, Art. no. 062343.

[246] P. Jouguet, D. Elkouss, and S. Kunz-Jacques, "High-bit-rate continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 90, Oct. 2014, Art. no. 042329.

[247] F. Furrer *et al.*, "Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks," *Phys. Rev. Lett.*, vol. 109, Sep. 2012, Art. no. 100502.

[248] F. Furrer, "Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle," *Phys. Rev. A*, vol. 90, Oct. 2014, Art. no. 042325.

[249] A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," *Phys. Rev. Lett.*, vol. 114, Feb. 2015, Art. no. 070501.

[250] P. Papanastasiou, C. Ottaviani, and S. Pirandola, "Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables," *Phys. Rev. A*, vol. 96, Oct. 2017, Art. no. 042332.

[251] X. Zhang *et al.*, "Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 96, Oct. 2017, Art. no. 042334.

[252] R. Arnon-Friedman, R. Renner, and T. Vidick, "Simple and tight device-independent security proofs," *arXiv:1607.01797*, 2016.

[253] D. Elkouss, J. Martinez-Mateo, and V. Martin, "Secure rate-adaptive reconciliation," in *Proc. Int. Symp. Inf. Theory Appl. (ISITA)*, Taichung, Taiwan, 2010, pp. 179–184.

[254] X. Wang *et al.*, "Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution," *Quant. Inf. Comput.*, vol. 17, nos. 13–14, pp. 1123–1134, 2017.

[255] X.-Q. Jiang, P. Huang, D. Huang, D. Lin, and G. Zeng, "Secret information reconciliation based on punctured low-density parity-check codes for continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 95, Feb. 2017, Art. no. 022318.

[256] L. Hanzo, T. H. Liew, B. L. Yeap, R. Y. S. Tee, and S. X. Ng, *Turbo Coding, Turbo Equalisation and Space-Time Coding: EXIT-Chart-Aided Near-Capacity Designs for Wireless Channels*, 2nd ed. New York, NY, USA: Wiley, 2011.

[257] C. Nguyen, G. Van Assche, and N. J. Cerf, "Side-information coding with turbo codes and its application to quantum key distribution," in *Proc. Int. Symp. Inf. Theory Appl. (ISITA)*, Parma, Italy, 2004.

[258] N. Benletaief, H. Rezig, and A. Bouallegue, "Toward efficient quantum key distribution reconciliation," *J. Quantum Inf. Sci.*, vol. 4, no. 2, pp. 117–128, 2014.

[259] W. Y. Liu *et al.*, "Experimental free-space quantum key distribution with efficient error correction" *Opt. Express*, vol. 25, no. 10, pp. 10716–10723, 2017.

[260] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[261] P. Jouguet and S. Kunz-Jacques, "High performance error correction for quantum key distribution using polar codes," *Quantum Inf. Comput.*, vol. 14, nos. 3–4, pp. 329–338, 2014.

[262] J. Niset, J. Fiurasek, and N. J. Cerf, "No-go theorem for Gaussian quantum error correction," *Phys. Rev. Lett.*, vol. 102, no. 12, 2009, Art. no. 120501.

[263] S. L. Braunstein, "Quantum error correction for communication with linear optics," *Nature*, vol. 394, pp. 47–49, Jul. 1998.

[264] S. Lloyd and J.-J. E. Slotine, "Analog quantum error correction," *Phys. Rev. Lett.*, vol. 80, pp. 4088–4091, May 1998.

[265] S. L. Braunstein, "Error correction for continuous variables," *Phys. Rev. Lett.*, vol. 80, no. 18, pp. 4084–4087, May 1998.

[266] T. A. Walker and S. L. Braunstein, "Five-wave-packet linear optics quantum-error-correcting code," *Phys. Rev. A*, vol. 81, Jun. 2010, Art. no. 062305.

[267] M. M. Wilde, H. Krovi, and T. A. Brun, "Entanglement-assisted quantum error correction with linear optics," *Phys. Rev. A*, vol. 76, Nov. 2007, Art. no. 052308.

[268] J. Niset, U. L. Andersen, and N. J. Cerf, "Experimentally feasible quantum erasure-correcting code for continuous variables," *Phys. Rev. Lett.*, vol. 101, no. 13, 2008, Art. no. 130503.

[269] T. Aoki *et al.*, "Quantum error correction beyond qubits," *Nat. Phys.*, vol. 5, no. 8, pp. 541–546, 2009.

[270] M. Lassen *et al.*, "Quantum optical coherence can survive photon loss using a continuous-variable quantum erasure-correcting code," *Nat. Photon.*, vol. 4, no. 10, pp. 700–705, 2010.

[271] M. Lassen, A. Berni, L. S. Madsen, R. Filip, and U. L. Andersen, "Gaussian error correction of quantum states in a correlated noisy channel," *Phys. Rev. Lett.*, vol. 111, Oct. 2013, Art. no. 180502.

[272] S. Hao, X. Su, C. Tian, C. Xie, and K. Peng, "Five-wave-packet quantum error correction based on continuous-variable cluster entanglement," *Sci. Rep.*, vol. 5, Oct. 2015, Art. no. 15462.

[273] C. Eichler *et al.*, "Observation of two-mode squeezing in the microwave frequency domain," *Phys. Rev. Lett.*, vol. 107, Sep. 2011, Art. no. 113601.

[274] E. P. Menzel *et al.*, "Path entanglement of continuous-variable quantum microwaves," *Phys. Rev. Lett.*, vol. 109, Dec. 2012, Art. no. 250502.

[275] E. Flurin, N. Roch, F. Mallet, M. H. Devoret, and B. Huard, "Generating entangled microwave radiation over two transmission lines," *Phys. Rev. Lett.*, vol. 109, Oct. 2012, Art. no. 183901.

[276] S. Barzanjeh, M. Abdi, G. J. Milburn, P. Tombesi, and D. Vitali, "Reversible optical-to-microwave quantum interface," *Phys. Rev. Lett.*, vol. 109, no. 13, 2012, Art. no. 130503.

[277] R. Di Candia *et al.*, "Quantum teleportation of propagating quantum microwaves," *EPJ Quantum Technol.*, vol. 2, p. 25, Dec. 2015.

[278] M. Abdi, P. Tombesi, and D. Vitali, "Entangling two distant non-interacting microwave modes," *Annalen der Physik*, vol. 527, nos. 1–2, pp. 139–146, 2015.

[279] S. Barzanjeh *et al.*, "Microwave quantum illumination," *Phys. Rev. Lett.*, vol. 114, Feb. 2015, Art. no. 080503.

Nedasadat Hosseinidehaj received the B.S. degree in electrical engineering from the Isfahan University of Technology, Isfahan, Iran, in 2008, the M.S. degree in electrical engineering from Tarbiat Modares University, Tehran, Iran, in 2012, and the Ph.D. degree in electrical engineering from the University of New South Wales, Sydney, Australia, in 2017. She is currently a Post-Doctoral Research Fellow with the Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland, Brisbane, Australia. Her current research interests are in the areas of continuous-variable quantum communications, including quantum key distribution.

Zunaira Babar received the B.Eng. degree in electrical engineering from the National University of Science and Technology, Islamabad, Pakistan, in 2008, and the M.Sc. degree (with Distinction) and the Ph.D. degree in wireless communications from the University of Southampton, U.K., in 2011 and 2015, respectively. She is currently a Research Fellow with the Southampton Wireless Group, University of Southampton.

Her research interests include quantum error correction codes, channel coding, coded modulation, iterative detection, and cooperative communications.

Robert Malaney received the Bachelor of Science degree in physics from the University of Glasgow, and the Ph.D. degree in physics from the University of St. Andrews, U.K. He is currently an Associate Professor with the School of Electrical Engineering and Telecommunications, University of New South Wales, Australia. He has over 150 publications. He has previously held research positions with Caltech, University of California at Berkeley, National Labs, and the University of Toronto. He is a former Principal Research Scientist with CSIRO.

Soon Xin Ng (S'99–M'03–SM'08) received the B.Eng. degree (First Class) in electronic engineering and the Ph.D. degree in telecommunications from the University of Southampton, Southampton, U.K., in 1999 and 2002, respectively. From 2003 to 2006, he was a Post-Doctoral Research Fellow working on collaborative European research projects known as SCOUT, NEWCOM, and PHOENIX. Since 2006, he has been an Academic Staff Member with the School of Electronics and Computer Science, University of Southampton. He was involved in the OPTIMIX and CONCERTO European projects as well as the IU-ATC and UC4G projects. He was the Principal Investigator of an EPSRC project on Cooperative Classical and Quantum Communications Systems. He is currently an Associate Professor in telecommunications with the University of Southampton. His research interests include adaptive coded modulation, coded modulation, channel coding, space-time coding, joint source and channel coding, iterative detection, OFDM, MIMO, cooperative communications, distributed coding, quantum communications, quantum error correction codes, and joint wireless-and-optical-fiber communications. He has published over 240 papers and co-authored two Wiley/IEEE Press books in the above areas. He is a fellow of the Higher Education Academy in the U.K., a Chartered Engineer, and a fellow of IET.

Lajos Hanzo (M'91–SM'92–F'04) received the degree in electronics in 1976, the Doctorate degree in 1983, and the Honorary Doctorate degrees *(Doctor Honoris Causa)* from the Technical University of Budapest in 2009 and the University of Edinburgh in 2015. During his 40-year career in telecommunications he has held various research and academic posts in Hungary, Germany, and the U.K. Since 1986, he has been with the School of Electronics and Computer Science, University of Southampton, U.K., where he holds the chair in telecommunications. He has successfully supervised 112 Ph.D. students, co-authored 18 Wiley/IEEE Press books on mobile radio communications totalling in excess of 10 000 pages, published 1768 research contributions at IEEE Xplore, acted both as a TPC and the General Chair of IEEE conferences, presented keynote lectures, and has been awarded a number of distinctions. He is currently directing a 40-strong academic research team, working on a range of research projects in the field of wireless multimedia communications sponsored by industry, the Engineering and Physical Sciences Research Council, U.K., the European Research Council's Advanced Fellow Grant and the Royal Society's Wolfson Research Merit Award. He is an enthusiastic supporter of industrial and academic liaison and he offers a range of industrial courses.

He was the Editor-in-Chief of the IEEE Press and a Chaired Professor also with Tsinghua University, Beijing, from 2008 to 2012. He is also a Governor of the IEEE ComSoc and of IEEE VTS. He is a fellow of the Royal Academy of Engineering, the Institution of Engineering and Technology, and the European Association for Signal Processing. For further information on research in progress and associated publications please refer to http://www-mobile.ecs.soton.ac.uk.