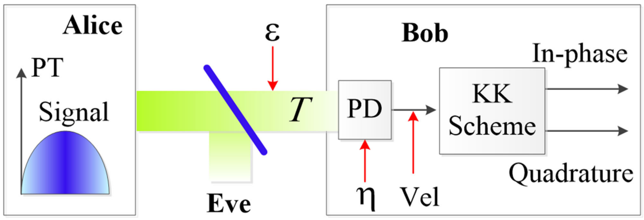
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

High-Speed Free-Space Optical Continuous Variable-Quantum Key Distribution Based on Kramers–Kronig Scheme

Volume 10, Number 6, December 2018

Zhen Qu, *Student Member, IEEE*
Ivan B. Djordjevic, *Senior Member, IEEE*



DOI: 10.1109/JPHOT.2018.2875590
1943-0655 © 2018 IEEE

High-Speed Free-Space Optical Continuous Variable-Quantum Key Distribution Based on Kramers–Kronig Scheme

Zhen Qu, ***Student Member, IEEE,***
and Ivan B. Djordjevic, ***Senior Member, IEEE***

Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ 85721 USA

DOI:10.1109/JPHOT.2018.2875590

Manuscript received September 26, 2018; accepted October 9, 2018. Date of publication October 11, 2018; date of current version October 29, 2018. This work was supported by the ONR MURI program (N00014-13-1-0627). Corresponding author: Dr. Zhen Qu (e-mail: zhenqu@email.arizona.edu).

Abstract: We propose and experimentally investigate a high-speed Kramers–Kronig (KK) scheme based continuous-variable quantum key distribution (CV-QKD) system over a free-space optical (FSO) channel. The atmospheric turbulence channel is emulated by three spatial light modulators on which three randomly generated azimuthal phase patterns yielding Andrews' spectrum are recorded. The proposed KK scheme enables a low-complexity implementation, insensitivity to laser phase noise, low detection noise, and accurate channel transmittance monitoring. In addition, eight state CV-QKD protocols and 10-channels wavelength-division multiplexing (WDM) scheme are experimentally verified to obtain a high secure key rate. In our experiment, the minimum transmittance of 0.6 is required to guarantee the secure transmission, and a total SKR of 2.1 Gb/s can be obtained at the mean transmittance in weak turbulence regime.

Index Terms: Continuous-variable quantum key distribution, discrete modulation, free-space optical communication, Kramers-Kronig scheme.

1. Introduction

Quantum key distribution (QKD) enables two legitimate parties, called "Alice" and "Bob", to share the key information with unconditional physical layer security. Recently, continuous-variable QKD (CV-QKD) protocols have attracted increasing attention, given that they are compatible with the commercially available telecom techniques, and potentially offer a high secure key rate (SKR) [1]. It has been widely believed that CV-QKD can only be implemented with homodyne detection, where only one quadrature component is measured at a time, or with heterodyne detection (HD), where one beam splitter (BS) and two homodyne detectors are used to measure both quadrature components simultaneously [2]. HD can double the mutual information (MI) at the expense of additional 3-dB loss of the BS. In order to reduce the laser phase noise after the coherent detection, the quantum signals are usually co-propagated together with the time-domain or frequency-domain multiplexed high-power pilot-tone (PT) to align Alice's and Bob's measurement bases [3], [4]. These approaches

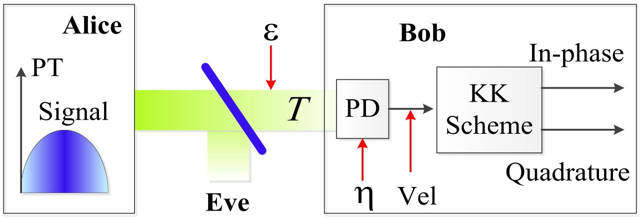


Fig. 1. Conceptual diagram of the proposed CV-QKD system based on KK scheme. ϵ: excess noise, V_{el}: electrical noise, T: Transmittance, η: detection efficiency.

are hard to implement in practice, impose limitations on the PT power, and lower down the spectral efficiency.

QKD implementations are usually deployed over free-space optical (FSO) links [5]. But the unknown transmittance fluctuation caused by atmospheric turbulence may bring the excessive post-processing noise [6]. Therefore, it is essential to accurately monitor the channel transmittance to guarantee uncompromised key security [7], [8]. In addition, most of the CV-QKD protocols are currently implemented based on Gaussian modulation, which in principle allow high SKR, but suffer low reconciliation efficiency [9]. Alternatively, discretely modulated CV-QKD protocols are also proposming solutions, which can leverage the state-of-the-art forward error correction (FEC) coding techniques [7]–[9]. Discretely modulated CV-QKD protocols have been proved to be unconditionally secure in linear quantum channels [10].

In this paper, for the first time, we propose and experimentally investigate a free-space optical CV-QKD system based on Kramers-Kronig (KK) scheme. The atmospheric turbulence channel is emulated by three spatial light modulators (SLMs) on which three randomly generated azimuthal phase patterns yielding Andrews' spectrum are recorded. The high-power PT is synchronized with the signal, multiplexed in frequency domain, and sent to Bob over the FSO channel. The commercial photodiode (PD) is employed at Bob's side and followed by the KK scheme to retrieve the phase information [11], [12]. As a consequence, both quadrature components of the incoming quantum signal can be measured simultaneously. Further, the detected PT power is used to monitor the channel transmittance. The proposed system combines the low-complexity advantage of the homodyne detection, double-MI advantage of the HD, accurate channel transmittance monitoring, low detection noise, and it is insensitive to the laser phase noise. We numerically and experimentally demonstrate that the eight-state CV-QKD protocol can achieve a high SKR in our proposed system.

The remainder of this paper is structured as follows. The CV-QKD system based on KK scheme is proposed and fully described in Section 2. In Section 3, the transmittance fluctuations, excess noise, and achievable SKRs are statistically measured and analyzed. In the end, the conclusions are provided in Section 4.

2. CV-QKD System Based on KK Scheme

Fig. 1 shows the conceptual diagram of the proposed CV-QKD system based on KK scheme. We denote the complex quantum signal by $s(t)$, whose spectrum is contained between $-B/2$ and $B/2$. The PT is assumed to be $E \exp(-j\pi B t)$, where E is a real and positive constant. It is well-known that minimum phase condition is required for phase retrieval in the KK scheme [11], i.e., $E > |s(t)|$. Assuming there is no channel loss and excess noise, the complex envelope of the field impinging on the PD is thus $r(t) = s(t) + E \exp(-j\pi B t)$. After the PD, the complex signal $s(t)$ can be reconstructed by the KK scheme. Because of the power of PT is far higher than that of the quantum signal, we have that $|r(t)| \approx E$. Therefore, the D.C. component after the PD detection, can be used to accurately monitor the power fluctuation caused by the atmopsheric turbulence effects in a FSO CV-QKD system. Compared to the HD scheme, where a BS will introduce extra 3 dB loss, the proposed KK scheme seperates the quadrature components in digital domain, and also successfully avoid the BS-induced 3 dB loss.

Under collective attacks, the asymptotic SKR based on reverse reconciliation is given as

$$\Delta I = \beta I_{AB} - \chi_{BE} \tag{1}$$

where β is the reconciliation efficiency, I_{AB} is the Shannon mutual information between Alice and Bob, χ_{BE} is the Holevo bound. According to the optimality of Gaussian attacks, the eight-state SKR definitions can be derived as [7], [13]

$$I_{AB} = \log_2 [(V + \chi_{tot}) / (1 + \chi_{tot})] \tag{2}$$

$$\chi_{BE} = G(\lambda_1) + G(\lambda_2) - G(\lambda_3) - G(\lambda_4) \tag{3}$$

with

$$\begin{aligned}
V &= V_A + 1, Z_{EPR} = \sqrt{V^2 - 1},\\
\chi_{tot} &= \chi_{line} + \chi_{KK}/T,\ \ \chi_{line} = 1/T + \epsilon - 1,\\
\chi_{KK} &= (1 + V_{el} - \eta)/\eta,\ \ T = T_0(Z_{DM}/Z_{EPR})^2,\\
\epsilon &= (Z_{EPR}/Z_{DM})^2(\epsilon_0 + V_A) - V_A,\\
G(x) &= \frac{(x+1)}{2}\log_2\left(\frac{(x+1)}{2}\right) - \frac{(x-1)}{2}\log_2\left(\frac{(x-1)}{2}\right),\\
\lambda_{1,2} &= \sqrt{\frac{1}{2}(A \pm \sqrt{A^2 - 4B})},\ \ \lambda_{3,4} = \sqrt{\frac{1}{2}(C \pm \sqrt{C^2 - 4D})},\\
A &= V^2 + T^2(V + \chi_{line})^2 - 2TZ^2_{\text{EPR}},\ \ B = (TV^2 + TV\chi_{line} - TZ^2_{\text{EPR}})^2,\\
C &= \frac{A\chi^2_{KK} + B + 1 + 2\chi_{KK}[V\sqrt{B} + T(V + \chi_{line})] + 2TZ^2_{\text{EPR}}}{[T(V + \chi_{tot})]^2},\\
D &= (V + \chi_{KK}\sqrt{B})^2[T(V + \chi_{tot})]^{-2}.
\end{aligned}$$

In the above expressions, Z_{DM} reflects the correlation between Alice and Bob modes in case of eight-state discrete modulation [7]. T_0 is the channel transmittance, ϵ_0 denotes the excess noise, V_{el} is the electrical noise at Bob's setup, and η is the detection efficiency. Notice that V_A, ϵ_0, and V_{el} are expressed in shot-noise units. In our system, we multiplex the PT and the signal by a relatively large frequency guard band, and send a high-power PT to meet the minimum phase condition, as well as to minimize the electrical noise V_{el}.

Assuming 6 GBaud eight-state modulated signals with $V_A = 0.5$ are prepared at Alice side and sent to Bob, under conditions of $V_{el} = 0$, $\eta = 0.8$, and $\beta = 0.9$, Fig. 2 shows the SKRs of the KK and the HD based CV-QKD systems in cases of $\epsilon_0 = 0$, 0.02, and 0.04. We can find that the proposed KK scheme can always outperform HD based scheme if there is no excess noise. In cases of $\epsilon_0 = 0.02$ and 0.04, KK scheme offers a higher SKR when the transmittance is larger than 0.24 and 0.85, respectively. When the the target SKR is 1 Gb/s, only KK scheme allows a secure communication with the transmittance higher than 0.72.

3. Experimental Results and Analysis

Fig. 3 shows the KK scheme based eight-state CV-QKD experimental setup. At Alice's side, the continuous wave (CW) light beams on a 50-GHz grid (193.15–193.6 THz) are generated from ten integrable tunable laser assembly (ITLA) lasers with a linewidth less than 10 kHz. The ten wavelength channels are multiplexed and sent to a dual-polarization-I/Q modulator (DP-IQM). A digital sequence of 6 GBaud eight-phase shift keying (8-PSK) symbols are generated and pulse shaped by a pair of root-raised-cosine filters with a roll-off factor of 0.5. The complex PT with 6 GHz RF is also generated in digital domain. The real and imaginary parts of the signal and PT are sent to the 10-bit resolution arbitrary waveform generator (AWG), which is operated at 25 GSa/s sampling

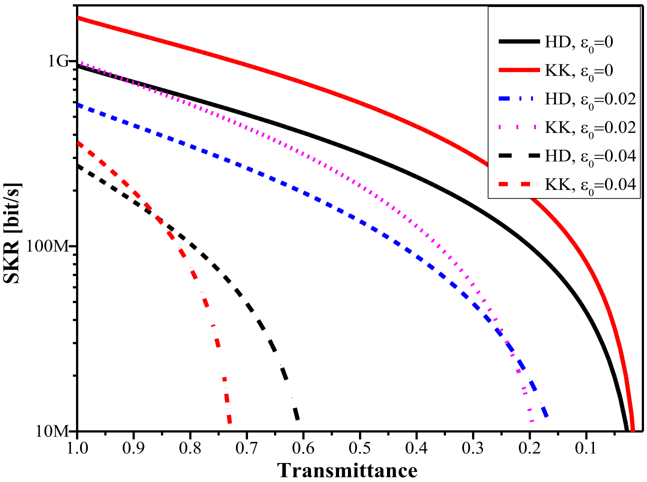


Fig. 2. SKR as a function of transmittance in KK scheme and HD based CV-QKD systems.

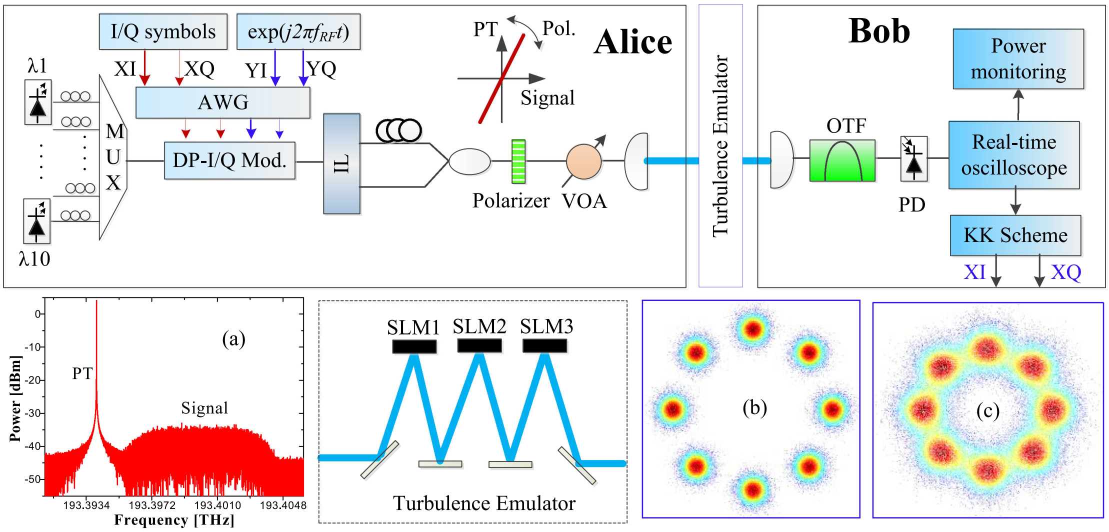


Fig. 3. Experimental setup. Inset: (a) The optical spectrum after the polarizer, (b) Recovered 8-PSK signal in case of high SNR value, (c) Recovered 8-PSK signal in case of low SNR value.

rate, and then drives the DP-IQM biased at null point. We use a modulator bias controller (MBC) to continuously track the bias drift and lock the null point. The signal and PT are synchronized and loaded onto the orthogonal polarizations of the CW light beam, then passed through a 50/100-GHz optical interleaver (IL) to separate the odd and even subchannels. The odd and even channels are then decorrelated by several hundreds of symbols via additional optical fiber and combined using a 3-dB coupler. The decorrelated WDM 8-PSK optical signals go through a polarizer and a variable optical attenuator (VOA). The polarizer is used to adjust the power ratio between the PT and signal, which is more than 1000:1, while the VOA is applied to easily control the total output power from Alice's side. Notice that this DP-IQM based PT/signal generation configuration is more complex than traditional IQM based schemes [12], but the signal and PT can be generated separately with higher quality. A typical optical spectrum after the polarizer is shown in inset of Fig. 3(a).

The optical beam is collimated to Gaussian beam, and then transmitted over the turbulence emulator. The atmospheric turbulence channel is emulated by SLMs on which three randomly

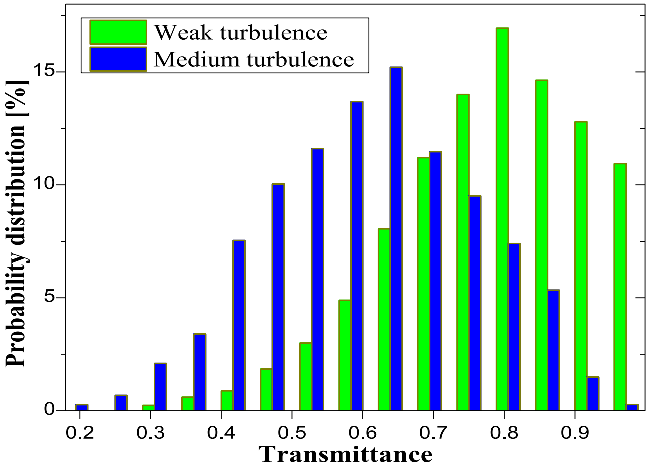


Fig. 4. Probability distribution of the fluctuating channel transmittances.

generated azimuthal phase patterns yielding Andrews' spectrum are recorded [14]. Note that the used SLMs offer 1920 × 1080 pixels' resolution, 15.36 mm × 8.64 mm active area, and 60 Hz image frame rate. The time-varying atmospheric turbulence is emulated by changing the random phase patterns at 50 Hz rate. This turbulence model is built on the weak turbulence environment (Rytov variance of $\sigma_R^2 = 0.02$), and the medium turbulence environment (Rytov variance of $\sigma_R^2 = 0.2$).

At Bob's side, the incoming beam is collected and out of which the central wavelength channel is selected by an optical tunable filter (OTF) with a 3 dB bandwidth of 12.5 GHz. The photocurrent is generated after the PD, and digitized by a real-time oscilloscope with 100 GSa/s sampling rate and 10-bit resolution. The KK scheme is then used to reconstruct the complex signal from the quantized intensity information. Insets of Fig. 3(b–c) show the recovered 8-PSK signal respectively, in cases of high and low SNR values. In our experiment, the electrical noise is very small, which is ~0.0013, because the PT power is far higher than the signal power. Bob's detection efficiency is measured to be $\eta = 0.65$.

Fig. 4 shows the monitored statistical distribution of the channel transmittance in weak and medium turbulence regimes. The mean transmittances are measured to be 0.78 and 0.61 for weak and medium turbulence conditions, respectively. Notice that the intrinsic transmittance loss in our turbulent model, e.g., the reflectivity of the SLM screens, is not considered here. It is because such intrinsic loss will not occur in real FSO channels.

We next measure the excess noise for a 1-hour time duration. When the modulation variance V_A is set to 0.5, Fig. 5 shows the excess noise of the proposed system as a function of time. The mean excess noise is measured to be 0.037 (in shot-noise units). Each point is measured with a block size of 106 points. The laser phase noise induced excess noise can be well eliminated by the KK scheme. The post-processing noise caused by the unknwon channel transmittance can also be negelected because we can accurately monitor the transmittance fluctuation. The excess noise consists of the quantization noise of the real-time oscilloscope, the modulation noise, and the relative intensity noise of the CW light source. In addition, part of the excess noise is contributed to the channel crosstalk from adjacent wavelength channels.

The experimentally measured SKRs in the proposed system are depicted in Fig. 6. We find that the minimum transmittance of 0.6 is required to obtain a secure communication. Given that the mean transmittances in our experiment are 0.61 and 0.78 for weak and medium turbulence conditions, respectively; secure communication is possible for both cases of interest in our experiment. More specifically, the SKR of 210 Mb/s per wavelength is achievable when the transmittance is 0.78. By summing up the SKRs obtained from 10 wavelength channels, the total SKR of 2.1 Gb/s can be achieved at the mean transmittance in case of weak turbulence. When the excess noise is mitigated well, the proposed system will enable secure communication at a lower channel transmittance.

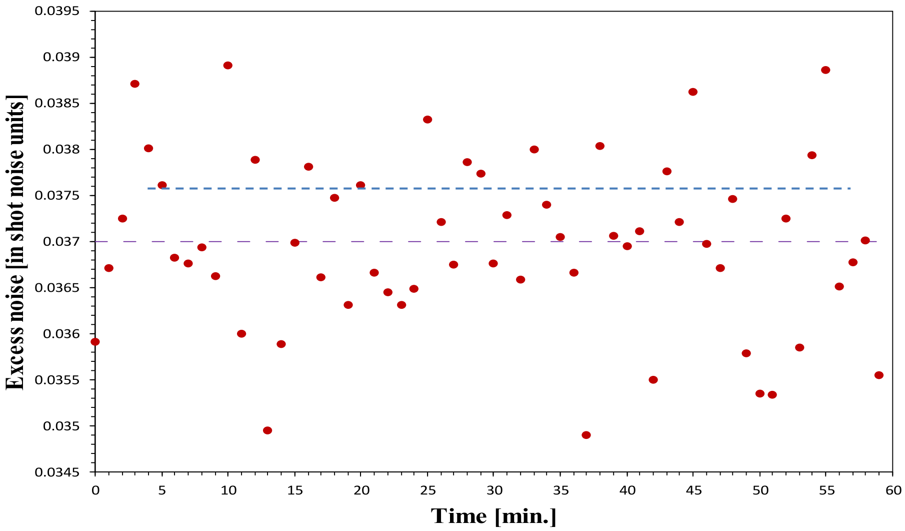


Fig. 5. Experimentally measured excess noise.

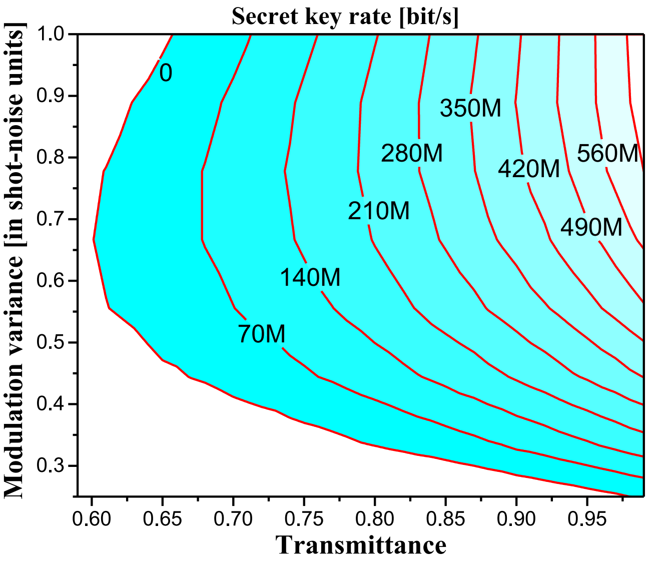


Fig. 6. Experimental SKRs as a function of the modulation variance and channel transmittance.

It is worthwhile to notice that the measured SKRs are calculated according to Eqs. (1)–(3) after the relevant system parameters are experimentally measured, e.g., channel transmittance, modulation variance, and detection efficiency. Therefore, the experimentally measured SKRs will agree well with the numerically calculated SKRs when same system parameters are used.

4. Concluding Remarks

We have proposed, theoretically analysed, and experimentally investigated a secure, compact, and high-speed eight-state FSO CV-QKD system based on KK scheme. The proposed protocol has been shown to achieve a high SKR, thanks to its insensitivity to the laser phase noise, transmittance monitoring and low detection noise featured KK scheme. Secure communication has been guaranteed in both weak and medium atmospheric turbulence regimes in our experiment, and a total SKR of 2.1 Gb/s has been experimentally achieved by using the WDM scheme at the mean transmittance in the weak turbulence regime.

To the authors' best knowledge, it is so far the simplest and lowest cost scheme that offer high tolerance to phase noise, detection noise, and channel transmittance fluctuation induced post-processing noise. In our simulation, heterodyne detection can outperform KK scheme in strong turbulence condition. While it is quite challenging to realize a perfect HD based CV-QKD system. For example, precise optical path alignment between the signal path and LO path is required to reduce the phase noise; low-temperature controlled photodiodes are usually used to reduce detection noise; channel transmittance is usually monitored by capturing a portion of the light by a beam splitter, which will introduce extra channel loss. In addition, only one PD is used for detection, which can avoid the security loophole caused by the imbalanced detection efficiency of the PDs in HD scheme. In the future, with more advanced techniques to suppress excess noise, KK scheme will play a more important role in CV-QKD commercial applications.

References

[1] S. L. Braunstein and P. Van Loock, "Quantum information with continuous variables," *Rev. Mod. Phys.*, vol. 77, pp. 513–577, 2005.

[2] F. Grosshans and N. J. Cerf, "Continuous-variable quantum cryptography is secure against non-Gaussian attacks," *Phys. Rev. Lett.*, vol. 92, 2004, Art. no. 047905.

[3] Z. Qu, I. Djordjevic, and M. A. Neifeld, "RF-subcarrier-assisted four-state Continuous-variable QKD Based on coherent detection," *Opt. Lett.*, vol. 41, no. 23, pp. 5507–5510, 2016.

[4] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection," *Phys. Rev. X*, vol. 5, 2015, Art. no. 041009.

[5] Z. Qu and I. B. Djordjevic, "Approaching Gb/s secret key rates in a free-space optical CV-QKD system affected by atmospheric turbulence," in *Proc. Eur. Conf. Opt. Commun.*, Gothenburg, 2017, Paper P2.SC6.32.

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

[7] Z. Qu and I. Djordjevic, "Four-dimensionally multiplexed eight-state continuous-variable quantum key distribution over turbulent channels," *IEEE Photon. J.*, vol. 9, p. 7600408, Dec. 2017, Art. no. 7600408.

[8] Z. Qu and I. Djordjevic, "High-speed free-space optical continuous-variable quantum key distribution enabled by three-dimensional multiplexing," *Opt. Exp.*, vol. 25, no. 7, pp. 7919–7928, 2017.

[9] A. Leverrier and P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation," *Phys. Rev. Lett.*, vol. 102, 2009, Art. no. 180504.

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

[11] A. Mecozzi, C. Antonelli, and M. Shtaif, "Kramers-Kronig coherent receiver," *Optica*, vol. 3, no. 11, pp. 1220–1227, 2016.

[12] X. Chen *et al.*, "218-Gb/s single-wavelength, single-polarization, single-photodiode transmission over 125-km of standard single-mode fiber using Kramers-Kronig detection," in *Proc. Opt. Fiber Commun. Conf.*, 2017, Paper Th5B.

[13] A. Becir, F. A. A. El-Orany, and M. R. B. Wahiddin, "Continuous-variable quantum key distribution protocols with eight-state discrete modulation," *Int. J. Quantum Inform.*, vol. 10, no. 1, 2012, Art. no. 1250004.

[14] Z. Qu and I. Djordjevic, "500 Gb/s free-space optical transmission over strong atmospheric turbulence channels," *Opt. Lett.*, vol. 41, no. 14, pp. 3285–3288, 2016.