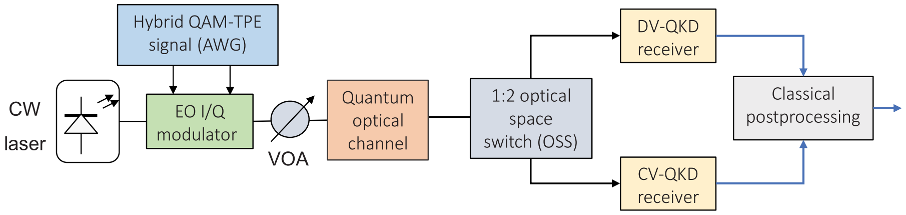
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Hybrid QKD Protocol Outperforming Both DV- and CV-QKD Protocols

Volume 12, Number 1, February 2020

Ivan B. Djordjevic



DOI: 10.1109/JPHOT.2019.2946910

Hybrid QKD Protocol Outperforming Both DV- and CV-QKD Protocols

Ivan B. Djordjevic

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

DOI:10.1109/JPHOT.2019.2946910

Manuscript received June 16, 2019; revised October 4, 2019; accepted October 9, 2019. Date of publication October 11, 2019; date of current version January 29, 2020. The work was supported in part by Multidisciplinary University Research Initiative (MURI) Office of Naval Research (ONR) under Project N00014-13-1-0627 and in part by the National Science Foundation under Grants 1907918 and 1828132.

Abstract: To overcome the limitations of both discrete variable (DV) and continuous variable (CV) QKD protocols, in this paper, a hybrid QKD protocol is proposed. In the proposed hybrid QKD protocol, Alice simultaneously performs discrete modulation (DM)-based encoding for CV-QKD subsystem and time-phase encoding for DV-QKD on a transmitter side and transmits such hybrid encoded pulse with optimized average number of photons per pulse. On receiver side, Bob employs a 1:2 optical space switch to select either DV-QKD receiver or CV-QKD receiver with the optimized probability of selection. Other compatible CV-QKD and DV-QKD protocols can also be used in hybrid QKD. Bob further performs the classical postprocessing applied to both subsystems so that resulting joint secure key is derived from both subsystems. The proposed hybrid QKD protocol significantly outperforms previously introduced both Gaussian modulation (GM)- and DM-based CV-QKD protocols as well as DV-QKD protocols in terms of both secret-key rate and achievable transmission distance.

Index Terms: Quantum communication, quantum key distribution (QKD), discrete variable (DV)-QKD, continuous variable (CV)-QKD, hybrid QKD, discrete modulation, decoy-state protocols, secret-key rate (SKR).

1. Introduction

The quantum key distribution (QKD) leverages the underlying principles of quantum information theory to realize the distribution of keys with verifiable security [1]–[3]. Thanks to the first satellite-to-ground QKD demonstration [4], recently, the research in QKD is getting momentum. The discrete variable (DV)-QKD scheme achieves the unconditional (perfect) security by employing no-cloning theorem and theorem on indistinguishability of arbitrary quantum states. The non-cloning theorem claims that arbitrary quantum states cannot be cloned, indicating that Eve cannot duplicate nonorthogonal quantum states even with the help of quantum computer. The second theorem claims that non-orthogonal states cannot be unambiguously distinguished. Namely, when Eve interacts with the transmitted quantum states, trying to get information on transmitted bits, she will inadvertently disturb the fidelity of the quantum states that will be detected by Bob. In contrast, the continuous variable (CV)-QKD employs the uncertainty principle claiming that both in-phase and quadrature components of a coherent state cannot be simultaneously measured with the complete precision. One of the key limitations for DV-QKD is the deadtime of the single-photon detectors (SPDs), ranging from 10 ns to 10 μs (depending on manufacturer), which limits the baud rate and, at the same time, the secret-key rate (SKR). Given that CV-QKD schemes employ the homodyne/heterodyne detection instead they do not exhibit the deadtime problem of the DV-QKD schemes.

The CV-QKD protocols can be categorized into two broad categories: (i) CV-QKD schemes based on finite-size signal constellations, known as the discrete modulation (DM) [5], [6], and (ii) CV-QKD schemes based on continuous Gaussian modulation (GM) [7]. The GM-based CV-QKD have very low information reconciliation (error correction) efficiency of corresponding practical error correction schemes [7]. On the contrary, DM-based CV-QKD protocols have excellent reconciliation efficiency and at the same time are compatible with commercial equipment for fiber-optics communications [3], [8]–[10]. As a such, they experience increasing research attention. Unfortunately, the strict security proofs of DM-based CV-QKD schemes for both collective and coherent attacks are still under development even though that some progress has been made recently [11].

To overcome these key challenges for DV-QKD, namely limited achievable transmission distance and low SKR values, as well as for DM-based CV-QKD, such as a nonexistence of strict security proofs, we propose here to employ a *hybrid DV-CV QKD protocol* to significantly increase SKR and extend the transmission reach. Standard DV-QKD protocols typically employ polarization states, time-bin encoding, phase encoding, and OAM modes, to mention few. However, polarization represents a fragile source of quantum information for transmission over optical fiber and long-distance free-space optical links. On the other hand, the time-bin and phase encodings are highly spectrally inefficient. The OAM modes are highly sensitive to the atmospheric turbulence effects. The key idea behind our hybrid DV-CV QKD protocol proposal is to employ DV-QKD subsystem to enable the unconditional security of DM-based CV-QKD subsystem as well. Given that key rates for CV-QKD subsystem is order of magnitudes higher than typical SKRs for DV-QKD subsystem, the DV-QKD subsystem does not need to be spectrally efficient, but instead be compatible with corresponding CV-QKD subsystem. So, we propose to employ the time-phase encoding for DV-QKD subsystem so that both polarization states can be employed in CV-QKD subsystem. In our proposed hybrid QKD protocol, Alice simultaneously performs DM-based encoding for CV-QKD subsystem and time-phase encoding for DV-QKD on transmitter side. On receiver side, Bob employs a 1:2 optical space switch to select either DV-QKD receiver or CV-QKD receiver with the optimized probability of selection, which is dependent on the SPD dead-time. Once the raw key transmission stage is completed, Bob will announce the instance of time when he employed CV- and DV-QKD receivers. Bob will then initiate the reverse reconciliation related to both subsystems, so that resulting secure key will be derived from both subsystems. In addition to the selected CV- and DV-QKD subsystems to be used in hybrid QKD, other compatible CV- and DV-QKD protocols are also applicable in hybrid QKD.

The paper is organized as follows. In Section 2, we describe the proposed hybrid QKD protocol. In the same section, we briefly describe how to calculate the SKR for any hybrid QKD protocol. In Section 3, we provide the illustrative SKR results. Finally, in Section 4, we provide some relevant concluding remarks.

2. Description of Proposed Hybrid QKD Protocol

The proposed generic prepare-and-measure (PM) hybrid DV-CV QKD protocol can be formulated as follows:

i) Alice creates at random one of M coherent states $|\alpha_k\rangle$ ($k = 0, 1, \ldots, M - 1$) with the help of a digital-to-analog converters (DACs) and an electrooptical I/Q modulator and locates them into at least one of N pulse positions. Such encoded hybrid DV-CV quantum state, in principle, can carry $N \times \log_2 M$ bits per photon. When both polarization states are employed, with the help of dual polarization I/Q modulator, the number of bits per transmitted pulse can be doubled. After the proper adjustment of the intensity, the hybrid quantum state is sent over the quantum channel such as fiber-optics channel or free-space optical (FSO) channel. For hybrid QKD system, the channel is characterized by the quantum bit-error rate (QBER) and transmissivity T. For CV-QKD subsystem, the channel is also characterized by the excess noise ε so that the total channel added noise, referred at the channel input, can be expressed in shot-noise unit (SNU) by $\chi_{\text{line}} = 1/T - 1 + \varepsilon$.

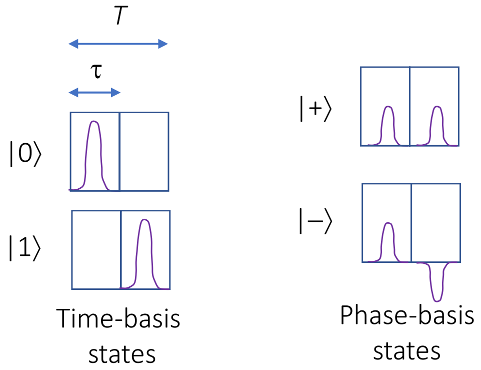


Fig. 1. The time-basis states and phase-basis states used in time-phase encoding for $N = 2$.

ii) On receiver side, Bob with the help of a 1:2 optical space switch (OSS) selects whether to use either DV-QKD receiver or CV-QKD receiver with optimized probability of selection, dictated by the dead time of SPDs. For time-phase encoding with $N = 2$, the DV-QKD receiver will be composed of a delay interferometer (DI) and two single-photon detectors (SPDs) of detection efficiency η_{d}. Regarding the CV-QKD receiver, Bob can perform either homodyne or heterodyne detection, with a detector being characterized by the detector efficiency η and electric noise variance v_{el}. Let the homodyne/heterodyne detection added noise variance referred to the Bob's input (channel output) be denoted as χ_{h}. For *homodyne detection*, we have that $\chi_{\mathrm{h}} = [(1 - \eta) + v_{\mathrm{el}}]/\eta$. On the other hand, for *heterodyne detection*, we have that $\chi_{\mathrm{h}} = [1 + (1 - \eta) + 2v_{\mathrm{el}}]/\eta$. Now the total noise variance for CV-QKD subsystem, referred at the channel input, can be expressed as $\chi_{\mathrm{total}} = \chi_{\mathrm{line}} + \chi_{\mathrm{h}}/T$.

iii) Once the transmission of sufficient number of symbols is completed, Bob will announce the instances of time when he employed CV- and DV-QKD receivers. Bob will then announce which symbol intervals should be used for QBER evaluation in both DV- and CV-QKD subsystems. For these locations, Bob will then disclose his measurements for both DV-QKD and CV-QKD subsystems, and Alice will calculate the corresponding overall QBER. If the QBER of hybrid DV-CV QKD system is below the prescribed threshold they continue with the protocol. (Otherwise, they abort the protocol.)

iv) Bob will then initiate the reverse reconciliation related to both subsystems, so that resulting corrected key will be derived from both subsystems jointly.

v) Finally, the privacy amplification will be performed to distil from corrected key a sequence of symbols whose correlation with Eve's sequence of symbols is below the desired threshold.

To solve for the photon number splitting (PNS) attack of the DV-QKD subsystem, we must employ the decoy-states-based approach. This indicates that Alice cannot employ M-ary PSK for her CV-QKD subsystem but star-QAM, square-QAM, cross-QAM, or iterative polar quantization (IPQ)-based signal constellation [12]–[14] instead. The star-QAM, also known as amplitude phase-shift keying (APSK), schemes are more suitable for this purpose, since optimized circle radii can be used corresponding to the signal and decoy states for DV-QKD subsystem. In that case, in CV-QKD modulator Alice will randomly select the circle (or equivalently signal/decoy state for DV-QKD subsystem) and then randomly select the constellation point to be used from that circle. Alice will further multiply such selected signal constellation point with the RF subcarrier. When the time-phase encoding [15] is employed in DV-QKD subsystem, Alice will transmit such generated symbol over randomly selected time slot of duration $\tau = T/N$ within the symbol duration T or in superposition state. As an illustration, the time-phase encoding basis states for BB84 protocol ($N = 2$) are provided in Fig. 1. The time-basis corresponds to the computational basis $\{|0\rangle, |1\rangle\}$, while the phase-basis to the diagonal basis $\{|+\rangle, |-\rangle\}$. The pulse is localized within the time bin of duration $\tau = T/2$. The time-basis is similar to the pulse-position modulation (PPM). The state in which the CV-modulated photon

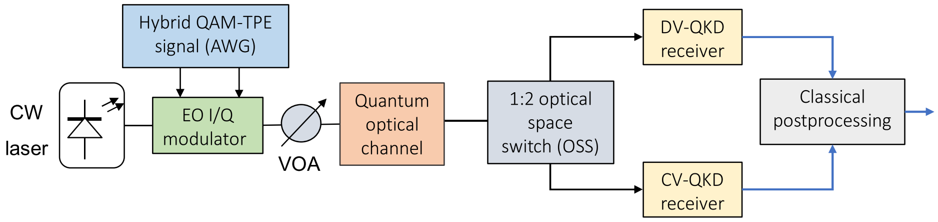


Fig. 2. The proposed hybrid DV-CV QKD scheme. TPE: time-phase encoding, AWG: arbitrary waveform generator, VOA: variable optical attenuator, and EO: electrooptical.

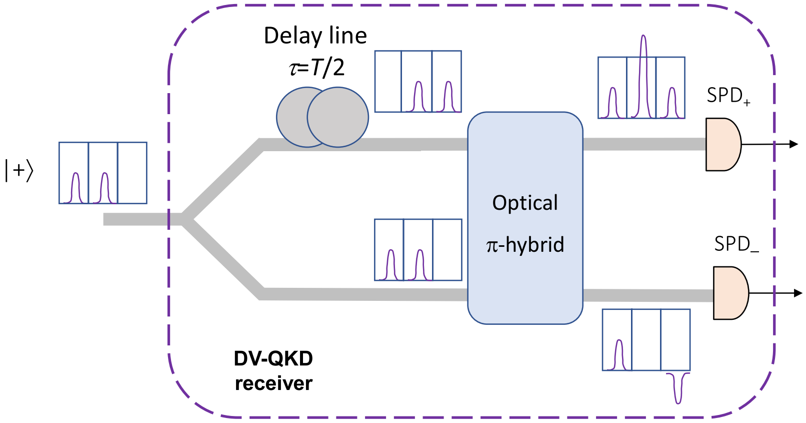


Fig. 3. The configuration of DV-QKD receiver for time-phase encoding.

is placed in the first-time bin (early state) is denoted by $|0\rangle = |e\rangle$, while the state in which the photon is placed in the second-time bin (late state) is denoted by $|1\rangle = |l\rangle$. The phase-basis states are defined by $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Alice randomly selects either the time-basis or the phase-basis, followed by random selection of the basis state. For DV-QKD subsystem, the logical 0 is represented by $|0\rangle$, $|+\rangle$; while logical one by $|1\rangle$, $|-\rangle$. The arbitrary waveform generator (AWG) is used to generate the corresponding RF waveforms as needed.

To implement this hybrid QKD protocol, we employ the generic scheme shown in Fig. 2. On Alice side, the APSK or IPQ symbols are first imposed on the RF subcarrier, then placed in corresponding time/phase basis states as described above, and such generated signal is then converted to the optical domain with the help of an electrooptical (EO) I/Q modulator and sent to Bob over either fiber-optics or FSO link. On receiver side, Bob employs a 1:2 optical space switch to select either DV-QKD receiver or CV-QKD receiver. The configuration of DV-QKD receiver for $N = 2$ is provided in Fig. 3. Time-basis states can be detected with the help of single SPD and properly designed electronics. On the other hand, to detect the phase-basis states, the time-delay interferometer can be used as shown in Fig. 3, composed of Y-junction at the input port and an optical π-hybrid, described by the scattering matrix $\boldsymbol{S} = [1\ 1;-1\ 1]/\sqrt{2}$ (see ref. [12]), at the output ports. The difference in the paths between two arms is $\Delta L = c\tau$ (c is the speed of light). When the phase-state $|+\rangle$ is incident to the time-phase decoder, the outputs of the π-hybrid occupy three-time slots, and the interferometer signals in the upper optical hybrid output branch interfere constructively, while at the lower output the corresponding signals interfere destructively. For constructive interference the middle pulse gets doubled, while for destructive interference middle pulses cancel each other. Therefore, the click of SPD in the middle slot at the upper output identifies the $|+\rangle$-state, while the corresponding click at the lower output identifies the $|-\rangle$-state.

The CV-QKD receiver, shown in Fig. 4, is based on the heterodyne coherent detection and employs the phase-noise compensation (PNC) module, which enables to reduce the level of excess

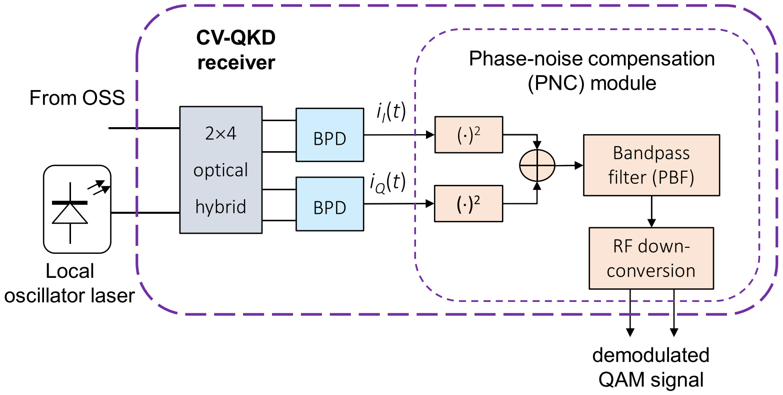


Fig. 4. The configuration of the RF-assisted CV-QKD receiver. BPD: balanced photodetectors.

noise [9]. The PNC module first squares the in-phase and quadrature signals, obtained after heterodyne detection takes place, and then either subtracts or adds these, which depends on the particular implementation of the optical hybrid type. The PNC module then performs bandpass filtering (BPF) to remove undesired double-frequency terms as well as the d.c. component. After that, the down-conversion is performed, which is typically implemented by two multipliers and low-pass filters (LPFs). Given that PNC module is capable of canceling the frequency-offset fluctuations as well as the laser phase noise, it is able to reduce the excess noise when compared to more traditional DM-based CV-QKD schemes. Of course, the traditional DM-based CV-QKD schemes, such as so-called distributed-phase-reference protocols, can alternatively be used for CV-QKD subsystem. The RF-assisted CV-QKD system is selected since it does not require the reference and as such it solves for potential security loophole problem of distributed-reference protocols. The CV-QKD receiver is provided for the completeness of presentation.

Once the key sifting phase is completed, the classical postprocessing steps take place, which are applied on both CV- and DV-QKD subsystems' raw keys, while the corresponding SKR, applicable to any hybrid QKD scheme, can be calculated as:

$$\begin{aligned} SKR &= R_{\text{raw}}\left[1-\text{leakage}_{\text{ECC}}(q)\right]-R_{\text{raw}}^{(\text{DV}-\text{QKD})}I_E^{(\text{DV}-\text{QKD})}-R_{\text{raw}}^{(\text{CV}-\text{QKD})}I_E^{(\text{CV}-\text{QKD})}, \\ R_{\text{raw}} &= R_{\text{raw}}^{(\text{DV}-\text{QKD})}+R_{\text{raw}}^{(\text{CV}-\text{QKD})} \end{aligned} \tag{1}$$

where $I_E^{(\text{DV}-\text{QKD})}(I_E^{(\text{CV}-\text{QKD})})$ is the mutual information that Eve was able to acquire on DV-QKD (CV-QKD) subsystem, and $R_{\text{raw}}^{(\text{DV}-\text{QKD})}(R_{\text{raw}}^{(\text{CV}-\text{QKD})})$ is the raw data rate between Alice and Bob related to the DV-QKD (CV-QKD) subsystem. We use $\text{leakage}_{\text{ECC}}(q)$ to denote the leakage of information due to error correction coding (ECC) under the assumption that overall QBER was q.

3. Illustrative Secret-Key Rates Results

In Fig. 5, we compare the proposed hybrid QKD protocol against the GM and eight-state DM protocols when typical reconciliation efficiencies are employed, wherein the output of optical switch is selected randomly. The CV-QKD subsystem is based on 8-star-QAM, with four points laying on inner circle and four point being on outer circle, with radiuses being optimally selected (to maximize the overall SKR). When optimized 8-star-QAM is used, the Holevo information between Bob and Eve is lower than corresponding Holevo information of GM, which results in higher SKRs than GM-based CV-QKD for the same reconciliation efficiency. The corresponding parameters are set as follows: the electrical noise variance is set to $v_{\text{el}}=10^{-2}$, the excess noise variance to $\varepsilon=10^{-3}$, and detector efficiency is set to $\eta=0.85$. On the other hand, for the DV-QKD subsystem, based on decoy-state BB84 protocol [16] with time-frequency encoding as described above, the parameters

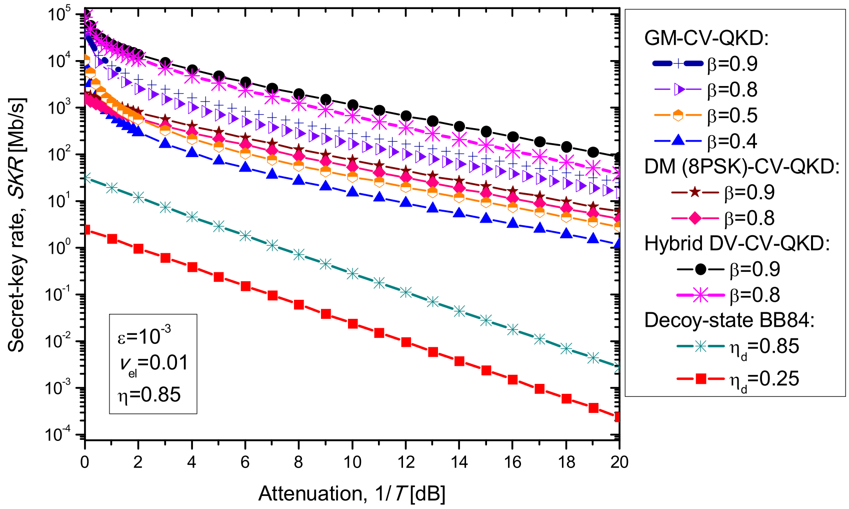


Fig. 5. The SKRs vs. the channel loss for proposed hybrid QKD scheme outperforming GM, eight-state CV-QKD, and decoy-state BB84 protocols. CV-QKD subsystem raw transmission rate was set to 10 Gb/s.

are being selected as follows: the deadtime of SPDs is set to 10 ns, the detection efficiency is $\eta_d = 0.85$, the intrinsic misalignment error rate is 0.005, the dark count rate is set to $p_d = 10^{-6}$, and the error correction (in)efficiency of decoy-state protocol is set to $f_e = 1.1$. In simulations, for the proposed hybrid QKD, the optimum average number of photons per pulse is used, obtained by maximizing the total SKR, assuming that information reconciliation is joint for DV- and CV-QKD subsystems. Evidently, when GM with typical reconciliation efficiency 0.5 is used it initially, for very low attenuation, outperforms the eight-state protocol (denoted as 8PSK protocol in the Figure) with reconciliation efficiency β ranging from 0.8 to 0.9. However, for medium and high channel losses, instead, the 8PSK protocol [8] outperforms the GM protocols with typical reconciliation efficiencies. On the other hand, the proposed hybrid QKD scheme significantly outperforms both GM and eight-state protocols in all attenuation regimes. For comparison purposes, we also provided the SKR results when decoy-state BB84 itself is used for two values of the detection efficiency 0.25 and 0.85. Clearly, the proposed hybrid QKD protocol outperforms the decoy-state BB84 for orders in SKR magnitude in all attenuation regimes. In the same figure, we provide comparison when GM-based CV-QKD protocol with reconciliation efficiency of 0.8 is used. Still the proposed hybrid QKD protocol, for the same reconciliation efficiency in CV-QKD subsystem, significantly outperforms the corresponding GM-based CV-QKD protocol.

In Fig. 6 we provide SKRs vs. transmission distance comparison of the proposed hybrid DV-CV-QKD protocol against that of GM and eight-state DM CV-QKD protocols assuming typical reconciliation efficiencies. The electrical noise variance is set to $v_{\mathrm{el}} = 0.01$, detector efficiency is $\eta = 0.85$, and excess noise variance is set to $\varepsilon = 10^{-3}$. For transmission medium, the ultra-low-loss fiber with attenuation coefficient $\alpha = 0.1419$ dB/km, described in [17], is assumed in calculations. Evidently, the proposed hybrid QKD protocol significantly outperforms both eight-state DM and GM protocols for both typical and the same reconciliation efficiencies, in terms of SKR vs. distance dependence. With proposed hybrid DV-CV-QKD protocol, the SKR of 1 Mb/s can be achieved for distance of 275 km, which represents the record SKR for this distance. It is interesting to notice that the proposed hybrid QKD and GM-based CV-QKD schemes have different slopes and they may eventually intersect at longer distances. However, operating the GM-based CV-QKD with SKRs well below 1 Mb/s is not very attractive for communication network applications because the corresponding memory unit storing the secure keys will quickly become empty when one-time pad is used, given huge disparity in typical bit rates used in optical communications and achievable SKRs.

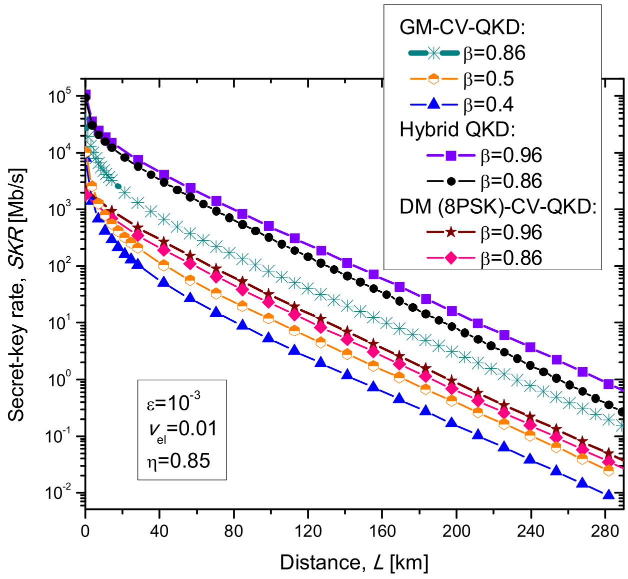


Fig. 6. The SKR vs. the transmission distance for proposed hybrid QKD scheme outperforming GM and eight-state CV-QKD protocols. The CV-QKD subsystem raw transmission rate was set to 10 Gb/s.

4. Concluding Remarks

In this paper, the hybrid DV-CV QKD protocol has been proposed to overcome the limitations of both DV and CV QKD protocols. In the proposed hybrid QKD protocol, Alice simultaneously performs DM-based encoding for CV-QKD subsystem and time-phase encoding for DV-QKD subsystem. On the other hand, Bob employs 1:2 optical space switch to select either DV-QKD receiver or CV-QKD receiver, followed by the classical postprocessing applied to both subsystems so that resulting joint secure key can be derived from both subsystems. The SKR results show that the proposed hybrid QKD protocol can significantly outperform CV- and DV-QKD protocols not only in terms of SKR, but also in terms of achievable transmission distance. To overcome the low-spectral efficiency of time-phase-encoding either Slepian states-based encoding [1] or OAM encoding [18] can be used instead; however, the complexity of such hybrid QKD system will be higher.

References

[1] I. B. Djordjevic, "FBG-based weak coherent state and entanglement assisted multidimensional QKD," *IEEE Photon. J.*, vol. 10, no. 4, Aug. 2018, Art. no. 7600512.

[2] S. Fossier *et al.*, "Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers," *J. Phys. B*, vol. 42, 2009, Art. no. 114014.

[3] Z. Qu and I. B. Djordjevic, "Four-dimensionally multiplexed eight-state continuous-variable quantum key distribution over turbulent channels," *IEEE Photon. J.*, vol. 9, no. 6, Dec. 2017, Art. no. 7600408.

[4] S.-K. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, pp. 43–47, 2017.

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

[6] R. Namiki and T. Hirano, "Security of quantum cryptography using balanced homodyne detection," *Phys. Rev. A*, vol. 67, 2003, Art. no. 022308.

[7] R. Garcia-Patron, "Quantum information with optical continuous variables: From Bell tests to key distribution," Ph.D. dissertation, Faculte des Sciences Appliquees, Université Libre de Bruxelles, Brussels, Belgium, 2007.

[8] A. Becir *et al.*, "Continuous-variable quantum key distribution protocols with eight-state discrete modulation," *Int. J. Quantum Inf.*, vol. 10, 2012, Art. no. 1250004.

[9] Z. Qu, I. B. 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, Dec. 2016.

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

[11] J. Lin, T. Upadhyaya, and N. Lütkenhaus, "Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution," Dec. 30, 2019. [Online]. Available: https://arxiv.org/pdf/1905.10896.pdf

[12] I. B. Djordjevic, *Advanced Optical and Wireless Communications Systems*. Cham, Switzerland: Springer International Publishing, 2017.

[13] I. B. Djordjevic, H. G. Batshon, L. Xu, and T. Wang, “Coded polarization-multiplexed iterative polar modulation (PM-IPM) for beyond 400 Gb/s serial optical transmission,” in *Proc. Conf. Opt. Fiber Commun. Nat. Fiber Optic Eng. Conf.*, San Diego, CA, Mar. 2010, Paper OMK2.

[14] H. G. Batshon, I. B. Djordjevic, L. Xu, and T. Wang, “Iterative polar quantization-based modulation to achieve channel capacity in ultrahigh-speed optical communication systems,” *IEEE Photon. J.*, vol. 2, no. 4, pp. 593–599, Aug. 2010.

[15] N. T. Islam, C. C.W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, “Provably secure and high-rate quantum key distribution with time-bin qudits,” *Sci. Adv.*, vol. 3, 2017, Art. no. e1701491.

[16] H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” *Phys. Rev. Lett.*, vol. 94, Jun. 2005, Art. no. 230504.

[17] Y. Tamura *et al.*, “The first 0.14-dB/km loss optical fiber and its impact on submarine transmission,” *J. Lightw. Technol.*, vol. 36, pp. 44–49, Jan. 2018.

[18] I. B. Djordjevic, “Multidimensional QKD based on combined orbital and spin angular momenta of photon,” *IEEE Photon. J.*, vol. 5, no. 6, Dec. 2013, Art. no. 7600112.