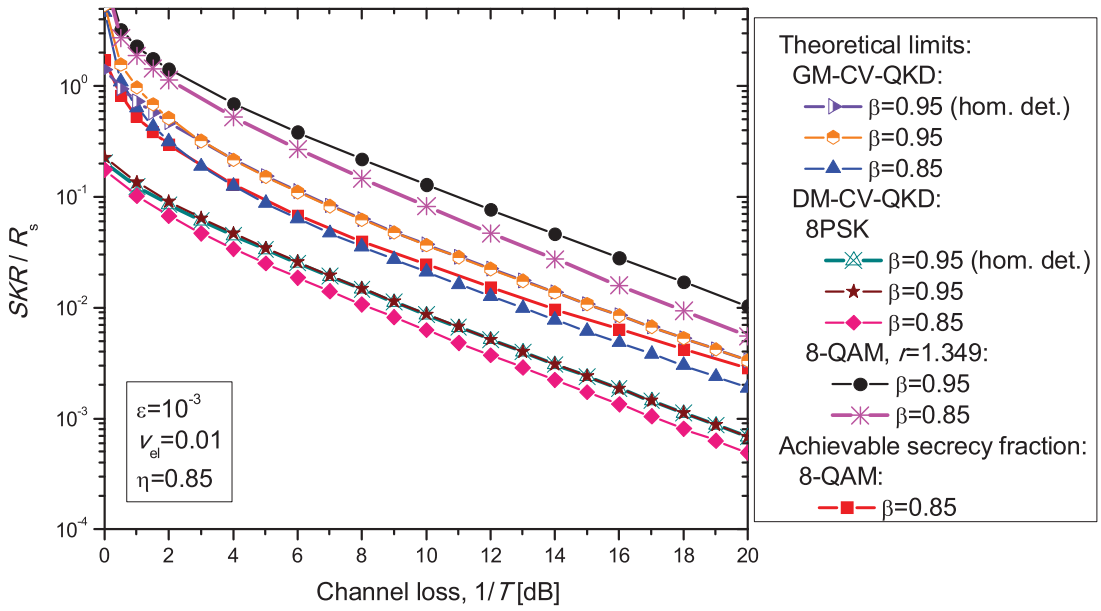
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Optimized-Eight-State CV-QKD Protocol Outperforming Gaussian Modulation Based Protocols

Volume 11, Number 4, August 2019

Ivan B. Djordjevic



DOI: 10.1109/JPHOT.2019.2921521
1943-0655 © 2019 IEEE

IEEE photonics SOCIETY

IEEE

Optimized-Eight-State CV-QKD Protocol Outperforming Gaussian Modulation Based Protocols

Ivan B. Djordjevic

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

DOI:10.1109/JPHOT.2019.2921521

Manuscript received April 19, 2019; revised May 28, 2019; accepted June 4, 2019. Date of publication June 6, 2019; date of current version June 27, 2019. The work was supported in part by the Multi-disciplinary University Research Initiative (MURI) Office of Naval Research (ONR) Project under Grant N00014-13-1-0627.

Abstract: In this paper, an optimized-eight-state CV-QKD protocol is proposed significantly outperforming previously introduced discrete modulation (DM) protocols as well as the corresponding Gaussian modulation (GM)-based CV-QKD protocols for practical reconciliation efficiencies values in terms of both secret-key rate (SKR) and achievable distance. The proposed CV-QKD protocol also outperforms, in terms of SKR, the corresponding high-cost single-photon DV-QKD scheme, employing an array of multiplexed single-photon detectors, for several orders of magnitude. We also describe a generalized RF-assisted CV-QKD scheme with heterodyne detection applicable to arbitrary DM scheme, insensitive to the laser phase noise and frequency offset fluctuations.

Index Terms: Quantum key distribution (QKD), continuous variable (CV)-QKD, prepare-and-measure CV-QKD protocols, discrete modulation-based protocols.

1. Introduction

IN recent years, the research in QKD is getting momentum [1]–[3], fueled by the first satellite-to-ground QKD demonstration [4]. One of the key limitations for discrete variable (DV)-QKD is the deadtime of the single-photon detectors (SPDs) employed in discrete variable (DV)-QKD, ranging from 10 ns to few μs (depending on manufacturer), which limits the signaling (raw) rate and therefore the secret-key rate (SKR). On the other hand, the continuous variable (CV)-QKD schemes do not exhibit the deadtime limitation problem, given that they employ either the homodyne or heterodyne detection instead.

The first CV-QKD protocols appeared in early 2000's and were based on discrete modulation (DM) [5], [6]. However, with occurrence of the Gaussian modulation (GM) the interest for DM went down. One of the key disadvantages of GM is low reconciliation efficiency of practical error correction schemes [7]. Recently, CV-QKD DM experiences re-surgency thanks to their simplicity for implementation and compatibility with the state-of-the fiber-optics communications' equipment [3], [8]–[10]. One of the key advantages of DM over GM is in availability of high reconciliation efficiency schemes, in particular those based on LDPC coding [11]. It has been shown in [12] that the reconciliation efficiency for DM schemes is much better than reconciliation efficiency for GM protocols. Another interesting observation originates from the information theory, which teach us that in very low signal-to-noise ratio (SNR) regime, which is a very common regime to CV-QKD

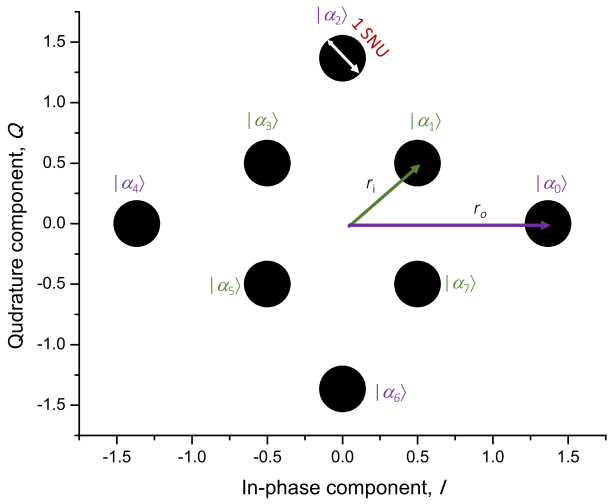


Fig. 1. The I-Q diagram for the proposed eight-state protocol.

schemes, the Shannon's channel capacity can be achieved even with small signal constellation sizes [11]. This idea was exploited in [7], [13] to show that in low SNR regime DM protocols can outperform corresponding GM protocols thanks to much better reconciliation efficiency. Moreover, by employing the radio frequency (RF)-assisted CV-QKD scheme proposed in [9], which is insensitive to the laser phase noise and frequency offset, the DM protocols with much lower excess noise can be employed, thus further outperforming GM protocols of bad reconciliation efficiency.

In this paper, we propose an optimized-eight-state CV-QKD protocol outperforming previously proposed DM protocols in terms of SKR as well as outperforming the GM CV-QKD schemes for practical reconciliation efficiencies values in terms of both achievable SKR and distance. The proposed scheme also significantly outperforms high-cost single-photon DV-QKD scheme with multiplexed SPDs for several order of magnitude in SKR. We also describe a generic RF-assisted CV-QKD scheme with heterodyne detection, representing the generalization of scheme introduced in [9], applicable to arbitrary DM-based CV-QKD scheme.

The paper is organized as follows. In Section 2, we describe the proposed optimized-eight-state CV-QKD protocol. In Section 3, we describe how to calculate the SKR of proposed optimized-eight-state-CV-QKD protocol. In Section 4, we provide the illustrative SKR results. Finally, in Section 5, we provide some relevant concluding remarks.

2. Proposed Optimized-Eight-State CV-QKD Protocol

The proposed optimized-eight-state prepare-and-measure (PM) protocol can be formulated as follows:

1) Alice sends at random one of eight coherent states $|\alpha_k\rangle = |\alpha_o \exp(jk\pi/4)\rangle$ $(k = 0, 2, 4, 6)$, $|\alpha_m\rangle = |\alpha_i \exp j[\pi/4 + (m-1)\pi/4]\rangle$ $(m = 1, 3, 5, 7)$ to Bob over the quantum channel. In this protocol, with corresponding I-Q signal constellation diagram being described in Fig. 1, four-points are placed on outer circle of radius r_o, while the remaining four points are placed on inner circle of radius r_i. Alice's modulation variance for points placed on inner circle (of radius r_i) is given by $v_{A,i} = 2\alpha_i^2$. On the other hand, the modulation variance of Alice for points placed on outer circle (of radius r_o) is given by $v_{A,o} = 2\alpha_o^2$. The ratio of outer-to-inner circles' radii $r = r_o/r_i$ is optimized so that the corresponding SKR expression is maximized. The channel is characterized by transmissivity T and excess noise ε so that the total channel added noise, referred at the channel input, can be expressed in shot-noise unit (SNU) by $\chi_{\text{line}} = 1/T - 1 + \varepsilon$.
2) On receiver side, once the coherent state is received, Bob can perform either homodyne or heterodyne detection, with a detector being characterized by the detector efficiency η and

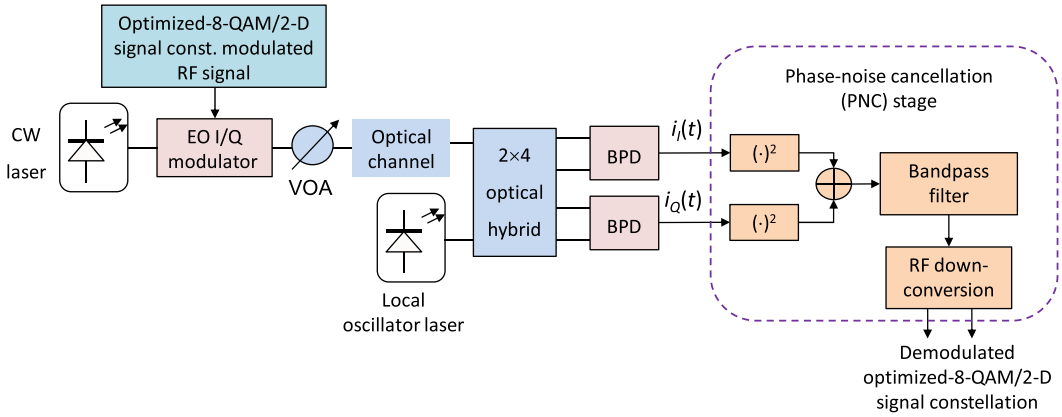


Fig. 2. The proposed optimized-eight-state RF-assisted CV-QKD scheme, which is also applicable to arbitrary 2-D constellation. VOA: variable optical attenuator, BPD: balanced photodetector, BPF: bandpass filter.

electric noise variance v_{el}. Let the detection added noise variance referred to the Bob's input (channel output) be denoted as χ_{h}. For *homodyne detection*, we have that $\chi_{\text{h}} = [(1-\eta) + v_{\text{el}}]/\eta$. On the other hand, for *heterodyne detection*, we have that $\chi_{\text{h}} = [1 + (1-\eta) + 2v_{\text{el}}]/\eta$. Now the total noise variance, referred at the channel input, can be expressed as $\chi_{\text{total}} = \chi_{\text{line}} + \chi_{\text{h}}/T$.

3) To implement this protocol, we employ the scheme shown in Fig. 2. On Alice side, the optimized 8-ary quadrature-amplitude modulation (8-QAM) signals are first imposed on the RF subcarrier and are then converted to optical domain with the help of an electrooptical (EO) I/Q modulator and sent towards Bob over either fiber-optics link or free-space optical (FSO) link. On receiver side, Bob employs the heterodyne coherent detection, combined with a phase-noise cancellation (PNC) stage to reduce the level of excess noise. The PNC stage first performs the squaring of the reconstructed in-phase and quadrature signals, followed by either addition or subtraction depending on the optical hybrid type. The PNC stage further performs bandpass filtering to remove DC component and double-frequency terms, followed by the down-conversion, implemented with the help of multipliers and low-pass filters (LPFs). Given that PNC stage removes the laser phase noise and frequency offset fluctuations, it exhibits better tolerance to the excess noise compared to the traditional DM-based CV-QKD schemes, since it is sensitive to the RF phase fluctuations only.
4) After the transmission process is completed, Alice announces which signalling intervals should be used for the detection of eavesdropping extent, and these symbols are not used for key generation. Given that the proposed scheme belongs to the class of discrete modulation schemes, similarly to DV-QKD, the extent of eavesdropping can be described in terms of bit-error rate (BER), which is easy to monitor. If the extent of eavesdropping (BER) is a below prescribed threshold they continue with the protocol. They then perform information reconciliation and privacy amplification in similar fashion as already in use for DV-QKD applications.

In the rest of this section, we describe the generic RF-assisted CV-QKD scheme, applicable to any two-dimensional (2-D) signal constellation, which represents the generalization of [9], which considers only *M*-ary phase shift keying (M-PSK) signals. The in-phase and quadrature components of RF-assisted either optimized-eight-state protocol or any 2-D signal constellation-based protocol can be represented as:

$$\begin{aligned} s_I(t) &= A\,\text{Re}\left\{[I(t) + jQ(t)]\exp(j\omega_{RF}t)\right\} = A\,I(t)\cos(\omega_{RF}t) - A\,Q\sin(\omega_{RF}t), \\ s_Q(t) &= A\,\text{Im}\left\{[I(t) + jQ(t)]\exp(j\omega_{RF}t)\right\} = A\,Q(t)\sin(\omega_{RF}t) + A\,Q\cos(\omega_{RF}t), \end{aligned} \quad (1)$$

where ω_{RF} is the RF radial frequency [rad/s], while $I(t)$ and $Q(t)$ represent the in-phase and quadrature coordinates of the RF signal. The modulation constant A is used to vary the modulation variance

of the signal v_A, typically expressed in SNU. For instance, for 8-PSK we have that $(I, Q) \in \{(1,0), (1/\sqrt{2}, 1/\sqrt{2}), (0, 1), (-1/\sqrt{2}, 1/\sqrt{2}), (-1, 0), (-1/\sqrt{2}, -1/\sqrt{2}), (0,-1), (1/\sqrt{2}, -1/\sqrt{2})\}$. For 8-QAM, the constellation diagram is provided in Fig. 1. The RF signal can be generated with the help of an arbitrary waveform generator (AWG). By biasing both in-phase and quadrature branches of the EO I/Q modulator at $\pi/4$-point (that is achieved by setting the DC voltage to $V_\pi/4$, where is the V_π is the half-wave switching voltage), the in-phase RF input of I/Q modulator can be written as $V_I(t) = (2/\pi)V_\pi s_I(t)$, while the quadrature RF input by $V_Q(t) = (2/\pi)V_\pi s_Q(t)$, so that the I/Q modulator output signal can be represented (in small signal analysis) as:

$$E_{\text{out}}(t) = \frac{1}{2}\sqrt{2P_s}e^{j[\omega_T t+\phi_T+\pi/4]} - A\ [I(t) + jQ(t)]\sqrt{P_s}e^{j[(\omega_T+\omega_{RF})t+\phi_T]}. \tag{2}$$

In Eqn. (2), P_s denotes the laser output power, ω_T is the transmit laser radial frequency, and ϕ_T represents the transmit laser phase noise.

On receiver side, when 2 × 4 optical hybrid, based on two Y-junctions and two 2 × 2 optical hybrids with properly selected phase trimers is used [11, Fig. 6.29], by squaring and subtracting the in-phase and quadrature photocurrents, denoted respectively as i_I and i_Q, followed by bandpass filtering (BPF) to remove the DC component and double-frequency terms, we obtain:

$$r(t) = BPF\left[i_I^2(t) - i_Q^2(t)\right] \Big/ \left(R^2P_sP_{LO}\sqrt{2}\right) \simeq AI(t)\cos(\omega_{RF}t - \pi/4) - AQ(t)\sin(\omega_{RF}t - \pi/4)$$
$$+\ n_{NB,I}\cos\omega_{RF}t - n_{NB,Q}\sin\omega_{RF}t, \tag{3}$$

where $n_{NB} = n_{NB,I} + j_{NB,Q}$ (in complex notation) denotes the equivalent narrowband noise at RF subcarrier level, P_{LO} denotes the power of local oscillator laser, and R denotes the photodiode responsivity. Evidently, from Eqn. (3) we see that the frequency offset $\omega_T - \omega_{LO}$ term as well as the phase noise term $\phi_T - \phi_{LO}$ are completely eliminated, indicating better tolerance of RF-assisted scheme to laser phase noise and frequency offset compared to the traditional CV-QKD schemes. Moreover, $\omega_T - \omega_{LO}$ must be sufficiently larger than ω_{RF} so that the beating component can be efficiently filtered out by BPF. This indicates that the RF-assisted scheme can only be used in heterodyne optical detection configuration. Now we perform the down-conversion process (multiplication followed by the LPFs) to obtain:

$$r_I(t) = LPF(r(t)2\cos(\omega_{RF}t - \pi/4)) \cong AI(t) + n'_I,$$
$$r_Q(t) = LPF(r(t)2\sin(\omega_{RF}t - \pi/4)) \cong -AQ(t) + n'_Q, \tag{4}$$

where n'_I and n'_Q are equivalent in-phase and quadrature low-pass additive noise processes. Clearly, the outputs of down-conversion block are proportional to in-phase and quadrature components of transmitted signal. Even though this scheme is described in context of 2-D modulation schemes, such as M-ary PSK and M-ary QAM, this scheme is also applicable to any higher-dimensional scheme.

3. Determination of SKR for Optimized-Eight-State CV-QKD Protocol

Given that in the PM DM protocol Alice sends the corresponding coherent states randomly, with the same probability, Bob will see the mixture states. The *mixture state* for the proposed *optimized-eight-state protocol* will be:

$$\hat{\rho} = \frac{1}{8}\sum_{k=0}^{7}|\alpha_k\rangle\langle\alpha_k|, \tag{5}$$

which can be expressed in terms of the $|\varphi_l\rangle$-states, defined as:

$$|\varphi_l\rangle = \frac{\exp\left[-\alpha^2/2\right]}{\sqrt{\zeta_l}}\sum_{n=0}^{\infty}\frac{\alpha^{8n+l}}{\sqrt{(8n+l)!}}|8n+l\rangle, \quad \alpha^2 = (\zeta_0+\zeta_2+\zeta_4+\zeta_6)\alpha_o^2 + (\zeta_1+\zeta_3+\zeta_5+\zeta_7)\alpha_i^2, \tag{6}$$

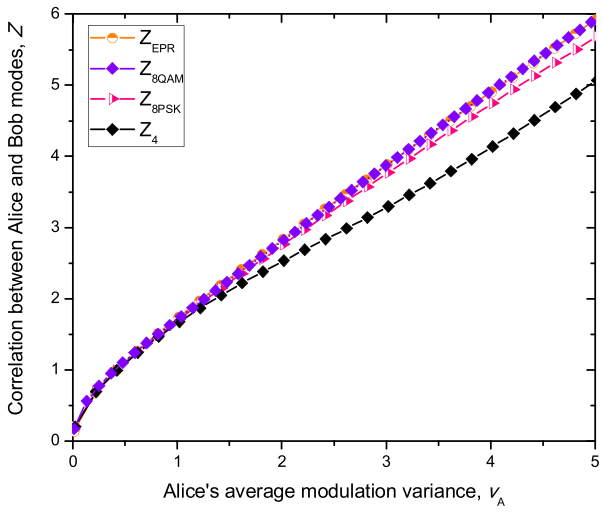


Fig. 3. The correlation between Alice and Bob's modes for various DMs against that for GM (Z_{EPR}) vs. Alice's average modulation variance v_A.

as follows:

$$\hat{\rho} = \sum_{l=0}^{7} \zeta_l \left|\varphi_l\right\rangle \left\langle\varphi_l\right|. \tag{7}$$

The coefficients ζ_l used in Eqns. (6) and (7) are determined by:

$$\begin{aligned}
\zeta_{0,4} &= C\exp\left(-\alpha_o^2\right)\left[\cosh\left(\alpha_o^2\right)+\cos\left(\alpha_o^2\right)\pm 2\cos\left(\frac{\alpha_o^2}{\sqrt{2}}\right)\cosh\left(\frac{\alpha_o^2}{\sqrt{2}}\right)\right],\\
\zeta_{2,6} &= C\exp\left(-\alpha_o^2\right)\left[\cosh\left(\alpha_o^2\right)-\cos\left(\alpha_o^2\right)\pm 2\sin\left(\frac{\alpha_o^2}{\sqrt{2}}\right)\sinh\left(\frac{\alpha_o^2}{\sqrt{2}}\right)\right],\\
\zeta_{1,5} &= C\exp\left(-\alpha_i^2\right)\left[\sinh\left(\alpha_i^2\right)+\sin\left(\alpha_i^2\right)\pm\sqrt{2}\cos\left(\frac{\alpha_i^2}{\sqrt{2}}\right)\sinh\left(\frac{\alpha_i^2}{\sqrt{2}}\right)\pm\sqrt{2}\sin\left(\frac{\alpha_i^2}{\sqrt{2}}\right)\cosh\left(\frac{\alpha_i^2}{\sqrt{2}}\right)\right],\\
\zeta_{3,7} &= C\exp\left(-\alpha_i^2\right)\left[\sinh\left(\alpha_i^2\right)-\sin\left(\alpha_i^2\right)\mp\sqrt{2}\cos\left(\frac{\alpha_i^2}{\sqrt{2}}\right)\sinh\left(\frac{\alpha_i^2}{\sqrt{2}}\right)\pm\sqrt{2}\sin\left(\frac{\alpha_i^2}{\sqrt{2}}\right)\cosh\left(\frac{\alpha_i^2}{\sqrt{2}}\right)\right],
\end{aligned} \tag{8}$$

wherein the normalization constant C is determined such that $\sum_{l=0}^{7}\zeta_l = 1$.

Following the similar approach to GM, the covariance matrix corresponding to joint Alice-Bob density state ρ_{AB} can be written as:

$$\Sigma_{AB} = \begin{bmatrix} (v_A+1)\mathbf{1} & \sqrt{T}Z_{DM}\boldsymbol{Z} \\ \sqrt{T}Z_{DM}\boldsymbol{Z} & \left[T\left(v_A+\varepsilon\right)+1\right]\mathbf{1} \end{bmatrix}, \tag{9}$$

where Z_{DM} is the correlation coefficient between in-phase and quadrature components for discrete modulation, v_A is Alice average modulation variance (in SNU), $\mathbf{1}$ is the 2×2 identity matrix, and $\boldsymbol{Z}$ is the Pauli-Z matrix, defined as $\boldsymbol{Z} = \mathrm{diag}(1, -1)$. As an illustration in Fig. 3, we show the behaviour of correlation terms Z_{DM} for four-state protocols Z_4, eight-state protocol introduced in [8], denoted as Z_{8PSK}; and the proposed optimized-eight-state protocol, denoted as Z_{8QAM}, against that for EPR state (denoted as Z_{EPR}) as a function of the average modulation variance of Alice, v_A. Evidently, for modulation variance $v_A \leq 1$, the Z_4 correlation term shows nice agreement with Z_{EPR}. On the other hand, for modulation variance $v_A < 5$, the Z_{8PSK} correlation term shows reasonably good agreement with Z_{EPR}. The correlation coefficient for the proposed protocol, Z_{8QAM}, shows an

excellent agreement for all values of v_A, when properly chosen outer-to-inner circle radii ratio r is employed.

Given that correlation coefficient between in-phase and quadrature components of proposed modulation scheme closely approaches the correlation coefficient for Gaussian modulation, the employment of modulation schemes of constellation sizes larger than eight will not bring any benefit compared to the proposed scheme. Moreover, from information theory we know that the channel capacity in low signal-to-noise ratio (SNR) regime, which is equivalent to high transmission loss regime in CV-QKD, can be achieved even with small signal constellation sizes.

Similarly to ref. [10], given an excellent agreement of Z_{8QAM} with Z_{EPR}, for any value of average Alice's variance, we could normalize the transmissivity T and redefine excess noise variance ε as follows:

$$T = \left(\frac{Z_{EPR}}{Z_{DM}}\right)^2 T', \quad \varepsilon = \left(\frac{Z_{DM}}{Z_{EPR}}\right)^2 (v_A + \varepsilon') - v_A \tag{10}$$

so that the corresponding correlation matrix between Alice and Bob becomes:

$$\Sigma_{AB} = \begin{bmatrix} (v_A + 1)\mathbf{1} & \sqrt{T'} Z_{EPR} \mathbf{Z} \\ \sqrt{T'} Z_{EPR} \mathbf{Z} & [T'(v_A + \varepsilon') + 1]\mathbf{1} \end{bmatrix}, \tag{11}$$

which is identical to the corresponding covariance matrix for Gaussian modulation, except for deferent transmissivity T' and excess noise variance ε' values. On such a way the expressions for SKRs derived earlier for GM (see for example ref. [2]) are directly applicable for DM as well. These transformations are also applicable to any higher order discrete modulation of size M as long as the correlation term Z_M has been determined first.

The expression for *secret fraction* (SF), obtained by *one-way postprocessing*, for reverse reconciliation, is given by:

$$SF = \beta I(A;B) - \max_{\text{Eve's strategies}} \chi(B;E), \tag{12}$$

where $I(A; B)$ is the mutual information between Alice and Bob, while the second term corresponds to the Holevo information between Eve and Bob, wherein the minimization of the SF is performed over all possible eavesdropping strategies. We use β to denote the reconciliation efficiency. For CV-QKD schemes, the secrecy rate can be interpreted as the normalized SKR, where the normalization is with respect to the signaling rate R_s. For the GM-based protocols the optimum eavesdropping strategy is a Gaussian attack [14]–[16]. For Gaussian channels, the mutual information between Alice and Bob is determined in the same fashion as for individual attacks:

$$I(A;B) = \frac{d}{2}\log_2\left(\frac{v + \chi_{\text{total}}}{1 + \chi_{\text{total}}}\right), \quad d = \begin{cases} 1, \text{ homodyne detection} \\ 2, \text{ heterodyne detection} \end{cases}, \tag{13}$$

The expression (13) is commonly used for DM-based protocols [10], [13], even though, strictly speaking, it is valid only for Gaussian source and Gaussian channel. For non-Gaussian sources, the corresponding secret fraction will represent an upper bound. In this paper we also employ the method to calculate $I(A; B)$ introduced in ref. [17], which is applicable to any DM scheme. The Holevo information between Bob and Eve, for heterodyne detection, is determined by [2], [10], [14], [16]:

$$\chi(B;E) = g\left(\frac{\lambda_1 - 1}{2}\right) + g\left(\frac{\lambda_2 - 1}{2}\right) - g\left(\frac{\lambda_3 - 1}{2}\right) - g\left(\frac{\lambda_4 - 1}{2}\right), \tag{14}$$

where $g(x) = (x + 1)\log_2(x + 1) = -x\log_2 x$ is the entropy of a thermal state with the mean number of photons being x. The λ-parameters are defined by [2], [10], [14], [16]:

$$\lambda_{1,2} = \sqrt{\frac{1}{2}\left(A \pm \sqrt{A^2 - 4B}\right)}, \quad \lambda_{3,4} = \sqrt{\frac{1}{2}\left(C \pm \sqrt{C^2 - 4D}\right)}, \tag{15}$$

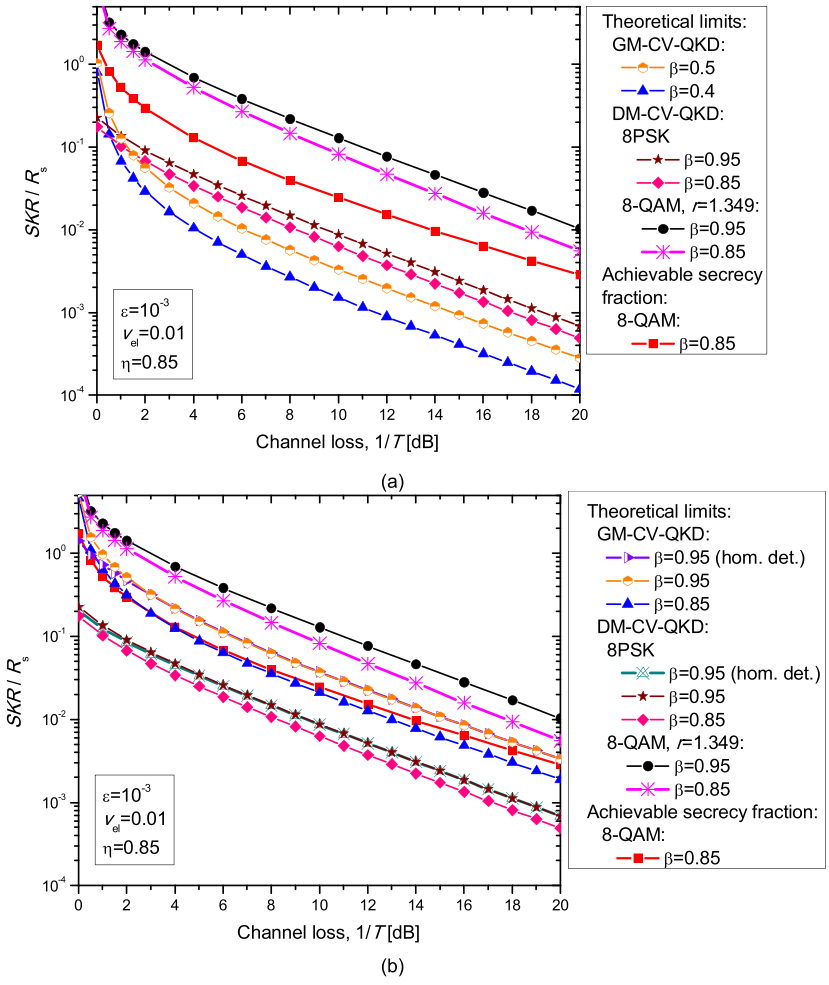


Fig. 4. The proposed optimized-eight-state CV-QKD scheme outperforming both GM and 8PSK CV-QKD protocols in terms of the normalized SKR vs. the channel loss for: (a) practical reconciliation efficiencies and (b) identical reconciliation efficiencies. R_s: the raw transmission rate.

where A, B, C, and D parameters are determined by [2], [10], [14], [16]:

$$A = v^2(1-2T') + 2T' + T'^2(v+\chi'_{\text{line}})^2,\ B = T'^2(1+T'v\chi'_{\text{line}})^2,$$

$$C = \frac{A\chi_{\text{het}}^2 + B + 1 + 2\chi_{\text{het}}\left[v\sqrt{B} + T(v+\chi'_{\text{line}})\right] + 2T(v^2-1)}{T^2(v+\chi'_{\text{total}})^2},\ D = \frac{\left(v+\chi_{\text{het}}\sqrt{B}\right)^2}{T^2(v+\chi'_{\text{total}})^2} \tag{16}$$

wherein $\chi'_{\text{line}} = 1/T' - 1 + \varepsilon'$, $\chi_{\text{het}} = [1+(1-\eta)+2v_{el}]/\eta$, $\chi'_{\text{total}} = \chi'_{\text{line}} + \chi_{\text{het}}/T'$, and $v = v_A + 1$, with v_A being the average Alice's variance.

4. Illustrative Secret-Key Rates Results

In Fig. 4(a), we compare the proposed optimized-eight-state protocol against previous DM and the GM protocols when practical reconciliation efficiencies are employed. In calculations, 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 $\eta = 0.85$. The reconciliation efficiency β is used as a parameter. In calculation, the ratio of outer-to-inner circles' radii $r = r_o/r_i$ is chosen to maximize the SKR, and optimum value for r is found to be 1.349. Evidently, when GM with reconciliation efficiency 0.5 is used it initially, for very low

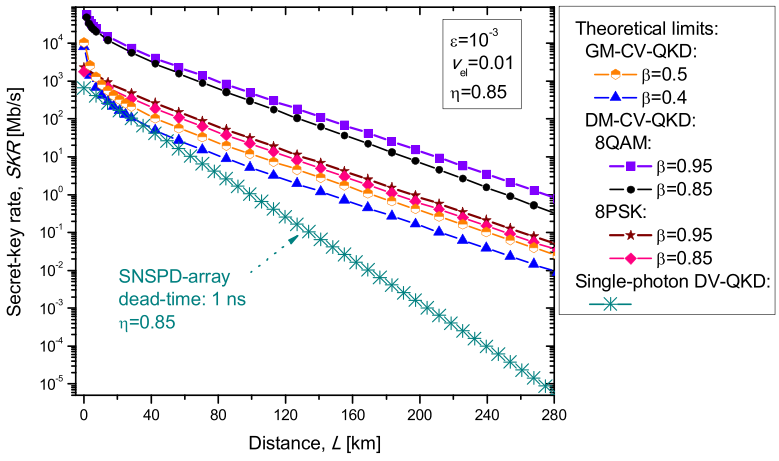


Fig. 5. The proposed optimized-eight-state CV-QKD scheme outperforming both GM and 8PSK CV-QKD in terms of SKR at a given distance for typical reconciliation efficiencies. The raw transmission rate for CV-QKD is set to 10 GS/s.

attenuation, outperforms the 8PSK protocol with β ranging from 0.85 to 0.95. However, for medium and high channel losses the 8PSK protocol significantly outperforms the GM protocols with typical reconciliation efficiencies. On the other hand, the proposed optimized-eight-state protocol, denoted in Figure as 8QAM theoretical limit, significantly outperforms both GM and 8PSK protocols in all attenuation regimes. In the same Figure we provide the achievable secrecy fraction, when mutual information $I(A; B)$ is calculated as described in [17]. Even though the gap to the upper limit in low and medium loss regimes is relevant, it reduces in high loss regime, and we conclude that the optimized-eight-state protocol still significantly outperforms other DM protocols as well the GM protocols.

On the other hand, in Fig. 4(b) we perform comparison for identical reconciliation efficiencies, even though these reconciliation efficiencies for the GM are quite difficult to achieve with reasonable complexity of corresponding error correction scheme. Nevertheless, the theoretical SKRs for the proposed DM scheme are significantly higher that SKRs for GM for the exactly the same reconciliation efficiencies. Given that the in-phase and quadrature components cannot be simultaneously measured, the homodyne detection has degradation in mutual information compared to corresponding heterodyne scheme. On the other hand, the 3 dB beam splitter is needed before heterodyne detection takes place, so that two schemes perform comparable as shown in Fig. 4(b), where homodyne and heterodyne detection schemes for GM and 8-PSK modulation with $\beta = 0.95$ are compared. In low-attenuation regime ($\leq$3 dB), the heterodyne detection slightly outperforms the homodyne detection scheme in SKR sense, which is a different trend from classical optical communications.

In Fig. 5 we provide SKR vs. transmission distance for proposed optimized-eight-state DM and GM protocols assuming typical reconciliation efficiencies. The electrical noise variance is set to $v_{\text{el}} = 0.01$, 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 [18], is assumed in calculations.

Evidently, the proposed optimized eight-state protocol significantly outperforms both 8PSK and GM protocols for typical reconciliation efficiencies, in terms of SKR vs. distance dependence. With proposed optimized eight-state DM protocol, the SKR of 1 Mb/s can be achieved for distance of 275 km, which represents the record SKR for this distance. This improvement can be contributed to improved mutual information of 8-QAM compared to 8-PSK, which is well documented in classical digital communications [19]. For comparison purpose, in the same Figure, we provide the SKR curve corresponding to single-photon DV-QKD scheme employing an array of multiplexed superconducting nanowire single-photon detectors (SNSPDs) of detector efficiency 0.85 [20]; with the

array effective dead-time being 1 ns that is implemented as described in [21]. Clearly, the SKR for proposed optimized-eight-state CV-QKD scheme is orders of magnitude higher compared to the high-cost single-photon DV-QKD scheme in all attenuation regimes. The SKR for DV-QKD can be improved by employing recently proposed phase matching twin-field (TF) QKD [22]. However, the TF-QKD concept is also applicable to CV-QKD schemes.

5. Concluding Remarks

An optimized-eight-state CV-QKD protocol has been proposed significantly outperforming both previously introduced DM protocols and GM-based CV-QKD protocols for practical reconciliation efficiencies in terms of the SKR for given channel attenuation and distance. As an illustration, high information reconciliation scheme proposed in [23] is directly applicable here, given that the proposed DM scheme belongs to the class of amplitude-phase-shift keying (APSK) modulation schemes. This information reconciliation scheme belongs to the class of low-complexity bit-interleaved coded modulation (BICM) and has already been implemented in FPGA. On the other hand, the same BICM-based information reconciliation scheme applied on GM cannot achieve the reconciliation efficiency higher than 0.5. To achieve higher reconciliation efficiencies, highly complex multistage decoding approach is required, such as one proposed in [24]. The multistage decoder in [24] was composed of two LDPC decoders and two BCH decoders, which might not be possible to be implemented on the same chip, in current ASIC technology. Moreover, the latency of the multistage decoding is huge compared to the BICM scheme.

For distance of 275 km, the SKR of 1 Mb/s is achievable with the proposed CV-QKD protocol, representing the record SKR for this distance. The corresponding high-cost single-photon DV-QKD, employing an array of multiplexed SNSPDs, can achieve the SKR of only 9 b/s for the same distance. The generalized RF-assisted CV-QKD scheme with heterodyne detection, applicable to arbitrary DM scheme, insensitive to the laser phase noise and frequency offset fluctuations, has been described as well.

The conventional DM/GM CV-QKD schemes are sensitive to the laser phase noise and frequency offset and as such exhibit high excess noise so that these record distances are not achievable. On the other hand, the proposed generalized RF-assisted CV-QKD employs the PNC stage which completely compensates the laser phase noise and frequency fluctuations and therefore has low excess noise so that long record distances are achievable. The corresponding experimental demonstration is straightforward as it represents just the generalization of the scheme we introduced in [3], [9]. The system complexity of proposed scheme is not much higher compared to conventional 8-PSK-based CV-QKD scheme proposed in [8]. Namely, to determine the shot noise level in spectral domain for any CV-QKD scheme, the use of RF subcarrier is required as described in [25].

As the final remark, the accurate proof for unconditional security for CV-QKD with DM for non-Gaussian channels is still an open problem, although there is some progress recently made as shown in [26].

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.
[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, Université Libre de Bruxelles, Bruxelles, 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] Y. Shen *et al.*, "Experimental study on discretely modulated continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 82, 2010, Art. no. 022317.
[11] I. B. Djordjevic, *Advanced Optical and Wireless Communications Systems*. New York, NY, USA: Springer, 2017.
[12] C. Weedbrook *et al.*, "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, 2012, Art. no. 621.
[13] 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.
[14] 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.
[15] F. Grosshans, "Collective attacks and unconditional security in continuous variable quantum key distribution," *Phys. Rev. Lett.*, vol. 94, 2005, Art. no. 020504.
[16] R. García-Patrón and N. J. Cerf, "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution," *Phys. Rev. Lett.*, vol. 97, 2006, Art. no. 190503.
[17] I. B. Djordjevic, "LDPC-coded MIMO optical communication over the atmospheric turbulence channel using Q-ary pulse-position modulation," *Opt. Exp.*, vol. 15, no. 16, pp. 10026–10032, Aug. 2007.
[18] 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, 2018.
[19] J. G. Proakis, *Digital Communications*. Boston, MA, USA: McGraw-Hill, 2001.
[20] I. E. Zadeh *et al.*, "Single-photon detectors combining high efficiency, high detection rates, and ultra-high timing resolution," *APL Photon.*, vol. 2, 2017, Art. no. 111301.
[21] S. A. Castelletto, I. P. Degiovanni, V. Schettini, and A. L. Migdall, "Reduced deadtime and higher rate photon-counting detection using a multiplexed detector array," *J. Mod. Opt.*, vol. 54, no. 2/3, pp. 337–352, 2007.
[22] X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," *Phys. Rev. X*, vol. 8, 2018, Art. no. 031043.
[23] D. Zou, C. Lin, and I. B. Djordjevic, "FPGA-based LDPC-coded APSK for optical communication systems," *Opt. Exp.*, vol. 25, no. 4, pp. 3133–3142, Feb. 2017.
[24] J. Lodewyck *et al.*, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Phys. Rev. A*, vol. 76, Oct. 2007, Art. no. 042305.
[25] Z.-Y. J. Ou, *Quantum Optics for Experimentalists*. London, U.K.: World Scientific, 2017.
[26] Z. Pan *et al.*, "Secret key distillation across a quantum wiretap channel under restricted eavesdropping." [Online]. Available: https://arxiv.org/abs/1903.03136