IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 21, 2019, accepted October 8, 2019, date of publication October 11, 2019, date of current version October 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2946777

On the Photon Subtraction-Based Measurement-Device-Independent CV-QKD Protocols

IVAN B. DJORDJEVIC, (Senior Member, IEEE)
Department of Electrical and Computer Engineering, The University of Arizona, Tucson, AZ 85721, USA
e-mail: ivan@email.arizona.edu

This work was supported in part by the NSF under Grant 1907918 and Grant 1828132.

ABSTRACT To potentially overcome the practical security loopholes of CV-QKD protocols, in this paper, we propose to use the optimized eight-state measurement-device-independent (MDI) protocol and demonstrate that it can significantly outperform corresponding Gaussian modulation-based MDI and virtual photon subtraction-based MDI CV-QKD protocols in terms of both secret-key rate and achievable transmission distance. Contrary to the common belief that virtual photon subtraction method can extend the distance of MDI CV-QKD protocols, we show that this is not true for fully optimized MDI CV-QKD protocols and realistic system parameters.

INDEX TERMS Quantum communication, quantum key distribution (QKD), continuous variable (CV)-QKD, Gaussian modulation, discrete modulation, measurement-device-independent (MDI) CV-QKD protocols, virtual photon subtraction method, secret-key rate (SKR).

I. INTRODUCTION

The quantum key distribution (QKD) leverages the principles of quantum mechanics to realize the distribution of keys with security that can be verified [1]–[8]. Various QKD schemes can be placed into two broad categories: discrete variable (DV) and continuous variable (CV) QKD schemes. DV-QKD employs the photon counting, followed by the postelection to identify signaling intervals when the detection takes place [7]. These schemes are affected by the long dead time of the single-photon detectors (SPDs), high dark current rate, and insufficient quantum efficiency. In contrast, the CV-QKD employs either homodyne or heterodyne detection. The long deadtime of SPDs, used in DV-QKD schemes, limits the baud rate and consequently the secret-key rate (SKR). Given that CV-QKD schemes employ the homodyne/heterodyne detection instead, they do not exhibit the deadtime problem. The CV-QKD protocols are typically implemented based on Gaussian modulation (GM) [9]–[14] or discrete modulation (DM) [15]–[19]. (An interested reader interested in differences between GM-based and DM-based CV-QKD schemes is referred to refs. [6] and [7].)

The associate editor coordinating the review of this manuscript and approving it for publication was Adnan M. Abu-Mahfouz.

The security analysis of CV-QKD schemes typically relies on idealized assumptions, which are very difficult to satisfy in practice. Any imperfection in practical devices yields to the security loophole that can be exploited by Eve to compromise security. Well known CV-QKD quantum attack strategies include: local oscillator fluctuation attack [20], LO wavelength attack [21], detection saturation attack [22], calibration attack [23], and the trojan horse attack on modulators [24], to mention few.

To overcome these practical security loopholes of CV-QKD protocols various measurement device-independent (MDI) CV-QKD protocols have been advocated [25]–[29]. The MDI QKD concept was first introduced in DV-QKD context to solve for various detector side-channel attacks [30], [31]. In MDI protocols [25]–[31], Alice and Bob are connected to a third party–Charlie, through corresponding quantum links (such as the free-space optical or the fiber-optics links). In MDI DV-QKD, Charlie performs partial Bell state measurement (BSM) with the help of a beam splitter (BS) and single-photon detectors and announces the results. In MDI CV-QKD, Charlie performs the dual-homodyne detection instead to determine in-phase and quadrature components and announces the results. In both versions, Alice and Bob simultaneously perform encoding and send the prepared quantum states toward the Charlie. Alice keeps her

quadrature components unchanged, while Bob updates them using Charlie's measurement results (with details provided later). While the employment of MDI concept can solve for detector side-channel attacks and simultaneously extend the transmission distance for DV-QKD, this is not the case for CV-QKD applications. The achievable transmission distances for symmetric MDI-based CV-QKD schemes, wherein Charlie is located in the middle of the link (at equal distances from Alice and Bob), is extremely short [28], [29]. To extend the transmission distance of symmetric MDI CV-QKD, the extreme asymmetric case has been introduced (see for example [28], [29]); however, the transmission distances are still shorter than that of conventional CV-QKD schemes. Another alternative to extend the transmission distance is to employ the virtual photon subtraction (PS) method [32]–[34].

In this paper, we study our previously proposed optimized eight-state DM protocol [35], called here optimized-8QAM, in MDI and virtual photon subtraction-based MDI CV-QKD settings. We demonstrate in Section V that the optimized eight-state MDI protocol can significantly outperform corresponding Gaussian modulation-based MDI and virtual photon subtraction-based MDI CV-QKD protocols in terms of both secret-key rate and achievable transmission distance. Contrary to the popular belief that virtual photon subtraction method can extend the transmission distance of MDI CV-QKD protocols, we demonstrate that this claim is not true for fully optimized MDI CV-QKD protocols.

The contributions of the paper can be summarized as follows: (i) contrary to the common belief we demonstrate that the photon subtraction deteriorates the performance of MDI CV-QKD schemes for optimized source variance and realistic system parameters, (ii) we show that the optimized 8QAM (opt8QAM)-based MDI scheme outperforms the GM-based MDI scheme, (iii) we demonstrate that the PS-based opt8QAM-MDI significantly outperforms other GM-based MDI CV-QKD schemes (in particular when the number of detected photons by the photon number resolution detector is zero), (iv) the corresponding channel matrices are derived and expressed in terms of equivalent channel noise variance rather than equivalent excess noise variance, (v) the PS-based MDI QKD for number of detected photons being zero is considered for the first time, (vi) we demonstrate that the employment of the photon subtraction module with number of detected photon being one is useful only for ideal system parameters, and (vii) the Gaussian source is implemented in electrical domain rather than optical domain.

The paper is organized as follows. In Section II, we describe a generic prepare-and-measure photon subtraction scheme-based MDI CV-QKD scheme that can be used for both DM and GM. Corresponding entanglement assisted scheme is described in In Section III. In the same section, we describe how to determine the covariance matrices for both GM and DM schemes. Both prepare-and-measure and entanglement assisted versions are described in terms of possible experimental demonstration. Section IV is devoted to the description of calculation of the SKRs. Some illustrative

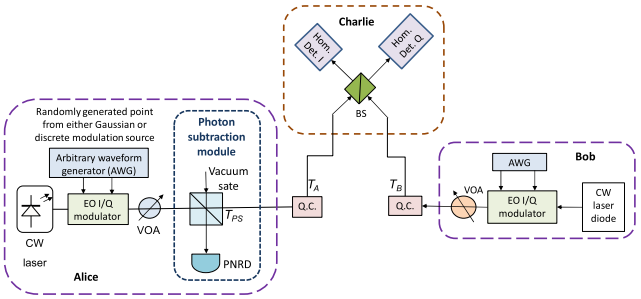

FIGURE 1. The prepare-and-measure photonic subtraction-based MDI CV-QKD scheme. VOA: variable optical attenuator, EO: electro-optical, PNRD: photon number resolving detector, BS: beam splitter, Q.C.: quantum channel.

SKR results are provided in Section V. Finally, some relevant concluding remarks are provided in Section VI.

II. PREPARE-AND-MEASURE PHOTON SUBTRACTION-BASED MDI CV-QKD SCHEME

The prepare-and-measure photonic subtraction-based MDI CV-QKD scheme under study in this paper, which is applicable to both GM and DM, is provided in Fig. 1. This scheme represents the generalization of MDI CV-QKD [28] and photon subtraction-based CV-QKD [32] schemes. For GM, Alice prepares the coherent state $|I_A + \mathrm{j}Q_A\rangle$, with the help of CW laser diode and an external electrooptical (EO) I/Q modulator, wherein the in-phase I_A and quadrature Q_A components of variance $v_A - 1$ are generated from two independent Gaussian sources in electrical domain, with the help of an arbitrary waveform generator (AWG), as illustrated in Fig. 1. The AWG outputs are used as RF inputs of the EO I/Q modulator. The E/O I/Q modulator can be replaced by the polar modulator, composed of concatenation of the Mach-Zehnder and phase modulators, which is a common practice in CV-QKD schemes. In a similar fashion, Bob prepares the coherent state $|I_B + \mathrm{j}Q_B\rangle$, wherein the in-phase I_B and quadrature Q_B components of variance $v_B - 1$ are generated from two independent Gaussian sources in electrical domain. For the discrete modulation case, Alice and Bob prepare each one of M coherent states selected at random, denoted as $|\alpha_k\rangle$ and $|\beta_m\rangle$, respectively ($k, m \in \{1, 2, \ldots, M\}$). When photon subtraction is employed, Alice further passes her coherent state through the *photon subtraction (PS) module* composed of the beam splitter (BS) of transmissivity T_{PS} and the photon number resolving detector (PNRD). The other BS output port is used as input to the PNRD. Alice and Bob then send such prepared coherent states towards Charlie over corresponding quantum channels. The PS module is applied only on Alice's side, since there is no advantage of putting it on Bob's side as shown in ref. [33]. Therefore, the key difference between the PS-based MDI CV-QKD scheme and MDI CV-QKD scheme is just in the PS module on Alice's side that is not needed in MDI CV-QKD scheme.

Charlie interferes two received modes, received from Alice and Bob, at his BS, followed by dual-homodyne

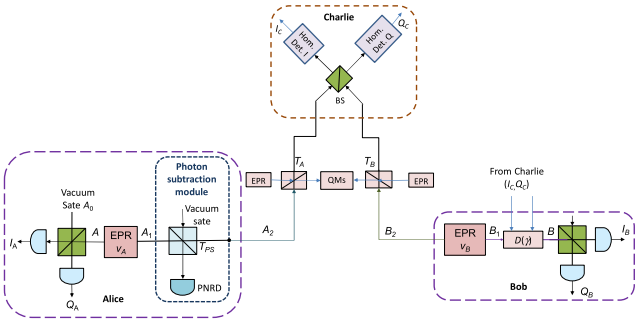

FIGURE 2. The equivalent entanglement assisted photonic subtraction-based MDI CV-QKD scheme. Two independent entangled-cloner attacks are applied by Eve. QM: quantum memories.

detection to determine the in-phase and quadrature components. Charlie then announces the results of dual-homodyne detection (I_C, Q_C). Alice keeps her in-phase and quadrature components unchanged, while Bob modifies his quadrature components as follows: $I'_B = I_B + \mu I_C$ and $Q'_B = Q_B - \mu Q_C$, where μ is the amplification coefficient to be determined in a similar fashion as described in [28].

When photon subtraction is employed, Alice announces signaling intervals when single photon is detected by her PNRD, and these signaling intervals are used in information reconciliation and privacy amplification stages. Other signaling intervals are ignored. When photon subtraction is not used, the conventional postprocessing is applied on all signaling intervals, except those used for parameter estimation.

It has been shown in a series of papers that the optimality of Gaussian attack is still applicable in this case (such as [31]–[33]), in particular for GM case. Even though non-Gaussian postelection is applied, the corresponding states being used during signaling stage are still Gaussian. Further, in this scenario Charlie is considered not trustworthy, and his detectors do not need to be perfect. This MDI CV-QKD protocol is tolerant to various side-channel attacks, listed in introduction.

In the next section, we describe the equivalent entanglement assisted protocols as well as how to determine the covariance matrices for both GM and DM-based MDI CV-QKD protocols under study.

III. THE EQUIVALENT ENTANGLEMENT ASSISTED PHOTON SUBTRACTION-BASED MDI CV-QKD SCHEME AND CORRESPONDING COVARIANCE MATRICIES

The corresponding equivalent entanglement assisted photonic subtraction-based MDI CV-QKD scheme is provided in Fig. 2, representing the generalization of CV-QKD scheme introduced in [33]. Alice and Bob generate two-mode squeezed (TMS) states with the help of the corresponding EPR source while keeping one mode each and sending the other towards Charlie, by employing two quantum channels at distances L_{AB} and L_{BC} from Charlie, respectively. When the photon subtraction method is employed, Alice passes the mode to be sent to Charlie first through the PS module. The modes received from Alice and Bob get interfered at Charlie's BS, followed by the dual-homodyne detection to determine in-phase and quadrature components (I_C, Q_C) and announces results. Bob then displaces his EPR mode B_1, described by the density operator $\hat{\rho}_{B_1}$, with the help of the displacement operation $D(\gamma)$, with γ being $g(I_C + jQ_C)$, where the g is the displacement gain. The resulting state after displacement can be represented by the following density operator $\hat{\rho}_B = D(\gamma)\,\hat{\rho}_{B_1} D^{\dagger}(\gamma)$. Alice and Bob then perform dual-homodyne measurements on their modes A and B to determine the corresponding in-phase and quadrature components. When the PS module is not employed, the conventional postprocessing (composed of information reconciliation and privacy amplification) is applied on all signaling intervals, except those used for parameter estimation. On the other hand, when the PS module is employed on Alice's side, Alice announces the signaling intervals where she detected single photon in her PS module and these signaling intervals are used in classical postprocessing to determine the secret key. Other signaling intervals are discarded.

In the absence of the PS module, following the procedure described in ref. [28], for GM case the covariance matrix $\sum_{AB}$ is given by:

$$\mathbf{\Sigma}_{AB} = \begin{bmatrix} v_A \mathbf{1} & \sqrt{T_c\left(v_A^2 - 1\right)}\mathbf{Z} \\ \sqrt{T_c\left(v_A^2 - 1\right)}\mathbf{Z} & T_c\left[v_A + \chi_{\text{line}}\right]\mathbf{1} \end{bmatrix}; \quad \mathbf{Z} = \text{diag}\,(1, -1), \quad \mathbf{1} = \text{diag}(1, 1), \tag{1}$$

where T_c is the equivalent channel loss given by $T_c = T_A g^2/2$ (with T_A being Alice-to-Charlie transmittance), while χ_{line} is the equivalent channel-added noise variance, expressed in shot-noise units (SNU), as follows:

$$\chi_{\text{line}} = \frac{1}{T_c} - 1 + \varepsilon, \tag{2}$$

with ε being the excess noise of the equivalent one-way protocol [28]:

$$\varepsilon = 1 + \frac{1}{T_A}\left[T_B\left(\chi_B - 1\right) + T_A \chi_A\right] + \frac{1}{T_A}\left(\frac{\sqrt{2}}{g}\sqrt{v_B - 1} - \sqrt{T_B\left(v_B + 1\right)}\right)^2. \tag{3}$$

In Eq. (3), T_A and T_B represent the transmittances of Alice-to-Charlie and Bob-to-Charlie channels, respectively. For fiber-optics-based channels, the corresponding transmittances are given by $T_A = 10^{-0.1\alpha L_{AC}}$ and $T_B = 10^{-0.1\alpha L_{BC}}$ respectively; where α is the fiber loss, which is 0.2 dB/km for standard single-mode fiber (SSMF) and 0.1419 dB/km for low-loss fiber [36]. Further, the Alice-to-Charlie and Bob-to-Charlie noise variances, denoted by χ_A and χ_B, respectively; are related to corresponding excess noise variances ε_A and ε_B by $1/T_A - 1 + \varepsilon_A$ and $1/T_B - 1 + \varepsilon_B$. By setting the gain coefficient such that the second term in (3) becomes 0, we obtain that $g = (2/T_B)^{1/2}[(v_B - 1)/(v_B + 1)]^{1/2}$. The corresponding

expression for the equivalent excess noise simplifies to

$$\varepsilon = \varepsilon_A + \frac{T_B}{T_A}(\varepsilon_B - 2) + \frac{2}{T_A}. \tag{4}$$

In a back-to-back configuration, when $T_A = T_B = 1$, we obtain that $\varepsilon = \varepsilon_A + \varepsilon_B$, indicating that the MDI CV-QKD will always perform worse than the conventional CV-QKD scheme.

The *symmetric case*, in which $L_{AC} = L_{BC}$, is limited to very short distances, as shown in [28]. The *extremely asymmetric case*, for which $L_{BC} \to 0$ and thus $T_B \to 1$, performs much better in terms of transmission distance and as such is considered in this paper. In high attenuation regime, $T_A << 1$, the MDI CV-QKD still performs worse compared to conventional CV-QKD given that in this case $\varepsilon \cong \varepsilon_A + \varepsilon_B/T_A >> \varepsilon_A$.

When the PS module is employed on Alice's side, based on ref. [32], we conclude that the corresponding covariance matrix for PS-based MDI CV-QKD can be written as:

$$\mathbf{\Sigma}_{AB} = \begin{bmatrix} V_A\mathbf{1} & \sqrt{T_c\eta_A\left(V_A^2-1\right)}\mathbf{Z} \\ \sqrt{T_c\eta_A\left(V_A^2-1\right)}\mathbf{Z} & T_c\eta_A\left[V_A+\chi'_{\text{line}}\right]\mathbf{1} \end{bmatrix},$$
$$V_A = 2\frac{k+1}{1-T_{PS}\frac{v_A-1}{v_A+1}} - 1, \tag{5}$$

where χ'_{line} and η_A are given respectively by:

$$\chi'_{\text{line}} = \frac{1}{\eta_A} - 1 + \frac{\chi_{\text{line}}}{\eta_A},$$
$$\eta_A = \frac{v_A-1}{v_A+1}T_{PS}\frac{k+1}{k+\frac{v_A-1}{v_A+1}T_{PS}}, \tag{6}$$

with k being the number of photons detected by Alice's PNRD.

For PS-based MDI CV-QKD with the *discrete modulation*, the corresponding covariance matrix is given by:

$$\mathbf{\Sigma}_{AB} = \begin{bmatrix} V_A\mathbf{1} & \sqrt{T_c\eta_A}Z_{DM}\mathbf{Z} \\ \sqrt{T_c\eta_A}Z_{DM}\mathbf{Z} & T_c\eta_A\left[V_A+\chi'_{\text{line}}\right]\mathbf{1} \end{bmatrix}, \tag{7}$$

where Z_{DM} is the correlation parameter dependent on DM scheme. As an illustration, Z_{DM} for 8PSK can be calculated as described in [17], while for optimized 8QAM the Z_{DM} parameter is determined in [35].

IV. THE SECRET-KEY RATE CALCULATION

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

$$SF = P_{PS}\left[\beta I(A;B) - \chi(B;E)\right], \tag{8}$$

where $I(A;B)$ represents the mutual information between Alice and Bob, while the second term $\chi(B;E)$ corresponds to the Holevo information between Eve and Bob. We use β to denote the reconciliation efficiency. For the GM with heterodyne detection the mutual information is calculated by:

$$I(A;B) = \log_2\left(\frac{V_A+\chi_{\text{total}}}{1+\chi_{\text{total}}}\right), \tag{9}$$

where $\chi_{\text{total}} = \chi'_{\text{line}} + \chi_{\text{het}}/T$ with χ_{het} representing the variance due to heterodyne detection being equal to $[1+(1-\eta)+2v_{\text{el}}]/\eta$, with η denoting the detector efficiency. The P_{PS} in Eq. (8) denotes the success probability when the PS module is used, which is determined by:

$$P_{PS} = \frac{1-\frac{v_A-1}{v_A+1}}{1-T_{PS}\frac{v_A-1}{v_A+1}}\left(\frac{1-T_{PS}}{\frac{v_A+1}{v_A-1}-T_{PS}}\right)^k, \tag{10}$$

where k denotes the number of photons detected by the photon number resolving detector.

The Holevo information between Bob and Eve, for heterodyne detection, is determined by [13]:

$$\chi(B;E) = g\left(\frac{\lambda_1-1}{2}\right) + g\left(\frac{\lambda_2-1}{2}\right) - g\left(\frac{\lambda_3-1}{2}\right) - g\left(\frac{\lambda_4-1}{2}\right), \tag{11}$$

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. Following the procedure described in [10]–[14], the λ-parameters are determined by:

$$\lambda_{1,2} = \sqrt{\frac{1}{2}\left(A \pm \sqrt{A^2-4B}\right)},$$
$$\lambda_{3,4} = \sqrt{\frac{1}{2}\left(C \pm \sqrt{C^2-4D}\right)}, \tag{12}$$

where A, B, C, and D parameters are determined in (13), as shown at bottom of this page, wherein $T = T_c\eta_A$, χ'_{line} has been introduced already by Eq. (6) and V_A is defined in Eq. (5).

$$A = V_A^2(1-2T) + 2T + T^2(V_A+\chi_{\text{line}})^2, \quad B = T^2\left(1+V_A\chi'_{\text{line}}\right)^2,$$
$$C = \frac{A\chi_{\text{het}}^2 + B + 1 + 2\chi_{\text{het}}\left[V_A\sqrt{B} + T\left(V_A+\chi'_{\text{line}}\right)\right] + 2T\left(V_A^2-1\right)}{T^2(V_A+\chi_{\text{total}})^2},$$
$$D = \frac{\left(V_A+\chi_{\text{het}}\sqrt{B}\right)^2}{T^2(V_A+\chi_{\text{total}})^2} \tag{13}$$

For PS-based MDI CV-QKD with the *discrete modulation*, the covariance matrix given by Eq. (7) has the standard form [6], [12] $\mathbf{\Sigma}_{AB} = \begin{bmatrix} a\mathbf{1} & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{1} \end{bmatrix}$, wherein $a = V_A$, $b = T(V_A + \chi'_{\text{line}})$, $c = T^{1/2}Z_{\text{DM}}$, so that A and B parameters needed in for Eq. (12) can be determined by:

$$A = a^2 + b^2 - 2c^2 = V_A^2 + T^2\left(V_A + \chi'_{\text{line}}\right)^2 - 2TZ_{DM},$$
$$B = (ab - c^2)^2 = T^2\left[V_A\left(V_A + \chi'_{\text{line}}\right) - Z_{DM}^2\right]^2. \quad (14)$$

On the other hand, following the procedure described in [6], [12] we determine the λ_3-parameter by:

$$\lambda_3 = \begin{cases} \sqrt{V_A\left(V_A - \dfrac{Z_{DM}^2}{V_A + \chi'_{\text{line}}}\right)}, & \text{for homodyne det.} \\ V_A - \dfrac{Z_{DM}^2}{V_A + \chi'_{\text{line}} + \dfrac{1}{T}}, & \text{for heterodyne det.} \end{cases} \quad (15)$$

while the λ_4-parameter is always 1.

V. ILLUSTRATIVE SECRET-KEY RATE RESULTS

In this section we study the SKR performance of optimized-8QAM (denoted as opt8QAM)-based MDI and PS MDI CV-QKD schemes, assuming that low-loss fiber of attenuation coefficient $\alpha = 0.1419$ dB/km, demonstrated in [36], is used. In opt8QAM four points are placed on circle of radius 1, while four points on circle of radius r. The maximization of SKR is performed with respect to the radius of outer circle and variances of the sources. For additional details related to the opt8QAM an interested reader is referred to our previous publication [35]. In all theoretical calculations, based on previous two sections [in particular Eqs. (5),(6),(8)-(15)], we assume that MDI schemes are extremely asymmetric ($L_{\text{BC}} = 0$ km) and based on Fig. 1. In Figure 3 we provide the SKR performance of opt8QAM-based MDI CV-QKD as a function of transmission distance, assuming that both Alice-to-Charlie and Bob-to-Charlie excess noise values are $\varepsilon_A = \varepsilon_B = 5 \times 10^{-4}$, while the detector efficiencies of both Charlies detectors are set to $\eta = 0.85$. The electrical variance of both in-phase and quadrature branches is set to $v_{\text{el}} = 10^{-2}$, while the information reconciliation efficiency is assumed to be $\beta = 0.85$. For comparison purposes the corresponding plots for GM and 8PSK-based MDI CV-QKD schemes are provided as well. Clearly, maximum transmission distances for 8PSK and GM-based MDI CV-QKD schemes are 86.6 km and 127.4 km, respectively. On the other hand the opt8QAM-based MDI CV-QKD scheme (for the radius of outer circle being $r = 1.349$) significantly outperforms both GM- and 8PSK-based MDI schemes in terms of SKR for all distances, and enables the maximum achievable distance of 165.1 km at SKR of 10 kb/s. Given that in high attenuation regime ($T_A << 1$), the equivalent excess noise can be represented $\varepsilon \cong \varepsilon_A + \varepsilon_B/T_A$, we conclude that it makes sense to invest in Bob-to-Charlie link to make excess noise ε_B as low as possible so that the achievable transmission distance can be extended. This scenario is also studied in Fig. 3, where we set ε_B to 10^{-5}, while ε_A is set to 10^{-3}. Clearly the transmission distance for GM- and opt8QAM-based MDI schemes can be extended to 235.7 and 259.3 km (also at SKR of 10 kb/s), respectively.

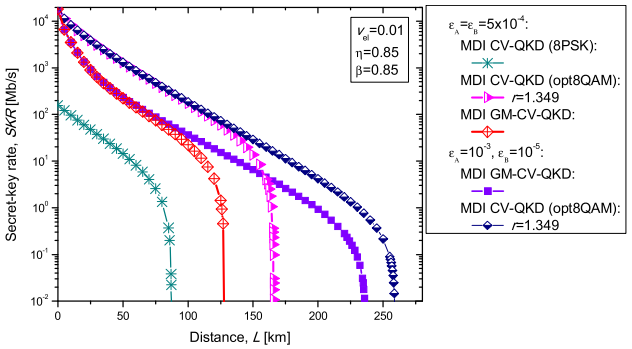

FIGURE 3. The opt8QAM-based MDI CV-QKD vs. GM-based MDI CV-QKD. The raw transmission rate is set to 10 Gb/s.

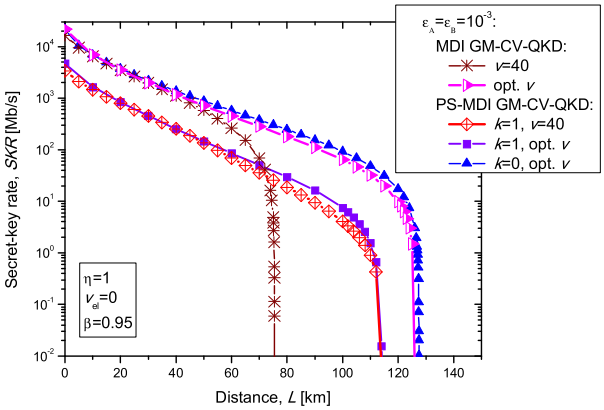

FIGURE 4. The PS MDI GM-CV-QKD vs. MDI GM-CV-QKD for the idealistic scenario. The raw transmission rate is set to 10 Gb/s.

In Figure 4, we study the SKR performance of GM-based MDI CV-QKD, with and without the PS module for two scenarios, when the variances of Alice and Bob sources is set to $v_A = v_B = v = 40$, the same as in [33]. (Notice that SSMF was used in [33], while the low-loss fiber is used here.) We also observe an *idealistic scenario* (similarly as in [33]), which is defined as the scenario for which the detector efficiency is ideal $\eta = 1$, electrical noise variance is negligible $v_{\text{el}} = 0$, and the reconciliation efficiency is close to 1, such as $\beta = 0.95$. Clearly, in this scenario the PS MDI scheme with $k = 1$ outperforms the conventional MDI scheme, in a similar fashion as predicted in [33]. However, when the same comparison is performed for the optimized source variance v (denoted in Figure as opt. v), which maximizes the SKR, the conventional MDI outperforms the PS-based (for $k = 1$) MDI for 12 km at SKR of 10 kb/s. Therefore, the PS module, for optimized source variance actually deteriorates both the SKR and achievable distance. For realistic system parameters, the optimum source variance that maximizes the SKR

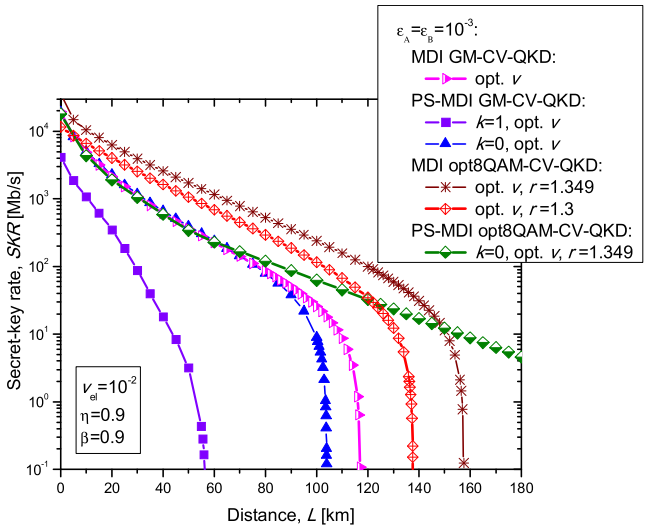

FIGURE 5. The opt8QAM-based PS MDI CV-QKD vs. GM-based PS MDI CV-QKD for realistic scenario. The raw transmission rate is set to 10 Gb/s.

is lower compared to the ideal case, so that the corresponding mutual information and the PS success probability get reduced, thus affecting overall SKR. Naturally there arises the question, whether the PS module for number of detected photons set to $k = 0$ be beneficial at all? In this case, the PNRD can be replaced by a single-photon detector (SPD), and Alice and Bob will use the signaling intervals when SPD does not detect the photon at all. This scenario is studied in Fig. 4 as well. Evidently, when the SPD was used in the PS module (for $k = 0$), the SKR performance of conventional MDI can be slightly improved; however, the achievable distance stays almost unchanged. The improvement for $k = 0$ case can be contributed to higher success probability in this scenario compared to the $k = 1$ case.

In Figure 5, we compare the PS-based MDI and conventional MDI performances for more realistic system parameters: the excess noise variances being $\varepsilon_A = \varepsilon_B = 10^{-3}$, the detectors' efficiencies set to $\eta = 0.9$, the electrical noise variance being $v_{\rm el} = 10^{-2}$, and the reconciliation efficiency set to $\beta = 0.9$. Clearly, for realistic system parameters, the conventional MDI with GM outperforms the PS-based MDI for both cases, when either PRND ($k = 1$) or SPD ($k = 0$) is used. The opt8QAM-based PS MDI QKD (for $k = 0$) significantly outperforms the GM-based PS MDI CV-QKD. Finally, the opt8QAM-based MDI significantly outperforms GM-based MDI in terms of SKR and can extend the transmission distance by 40.6 km at SKR of 10 kb/s. The PS-MDI for $k = 0$ outperforms MDI only when opt8QAM is used for distances above 160 km. However, in this case the number of subtracted photons is zero. This represents the only case when the use of the photon subtraction module is beneficial.

VI. CONCLUDING REMARKS

The use of opt8QAM-based MDI CV-QKD has been advocated in this paper to overcome various practical security loopholes of conventional CV-QKD protocols. We have demonstrated that the proposed opt8QAM-based MDI CV-QKD protocol can significantly outperform corresponding Gaussian modulation-based MDI and virtual photon subtraction-based MDI CV-QKD protocols in terms of both secret-key rate and achievable transmission distance. Contrary to the popular belief that virtual photon subtraction method can extend the distance of MDI CV-QKD protocols, we have shown that this is only true for idealistic system parameters. We have demonstrated that for optimized source variance and realistic system parameters, the photon subtraction method actually can deteriorate the SKR performance of MDI CV-QKD protocols and reduce the achievable transmission distance.

REFERENCES

[1] C. H. Bennet 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. [Online]. Available: https://s3.amazonaws.com/academia.edu.documents/30035361/bb84.pdf?response-content-disposition=inline%3B%20filename%3DQuantum_cryptography_Public_key_distribu.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20191012%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191012T193917Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=cd46b1d9507fba124c7a0165a353116eb999ca736de445c88a29e047f947e246

[2] C. H. Bennett CH, "Quantum cryptography: Uncertainty in the service of privacy," *Science*, vol. 257, pp. 752–753, Aug. 1992.

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

[4] G. van Assche, *Quantum Cryptography and Secrete-Key Distillation*. New York, NY, USA: Cambridge Univ. Press, 2006.

[5] 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.

[6] I. B. Djordjevic, *Physical-Layer Security and Quantum Key Distribution*. Cham, Switzerland: Springer, 2019.

[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lükenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, p. 1301, Sep. 2009.

[8] S. Guerrini, M. Chiani, and A. Conti, "Secure Key Throughput of Intermittent Trusted-Relay QKD Protocols," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–5.

[9] F. Grosshans and P. Grangier, "Reverse reconciliation protocols for quantum cryptography with continuous variables," Apr. 2002, *arXiv:quant-ph/0204127*. [Online]. Available: https://arxiv.org/abs/quant-ph/0204127

[10] C. Silberhorn, T. C. Ralph, N. Lutkenhaus, and G. Leuchs, "Continuous variable quantum cryptography: Beating the 3 dB loss limit," *Phys. Rev. Lett.*, vol. 89, no. 16, Sep. 2002, Art. no. 167901.

[11] M. Navascués, F. Grosshans, and A. Acín, "Optimality of Gaussian attacks in continuous-variable quantum cryptography," *Phys. Rev. Lett.*, vol. 97, no. 19, Nov. 2006, Art. no. 190502.

[12] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, p. 621, May 2012.

[13] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, "Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers," *J. Phys. B, At., Mol. Opt. Phys.*, vol. 42, no. 11, p. 114014, May 2009.

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

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

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

[17] 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, Feb. 2012, Art. no. 1250004.
[18] Y. Shen, H. Zou, L. Tian, P. Chen, and J. Yuan, "Experimental study on discretely modulated continuous-variable quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 82, Aug. 2010, Art. no. 022317.
[19] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 881–919, 1st Quart., 2019.
[20] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems," *Phys. Rev. A, Gen. Phys.*, vol. 88, Aug. 2013, Art. no. 022339.
[21] X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, "Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol," *Phys. Rev. A, Gen. Phys.*, vol. 87, May 2013, Art. no. 052309.
[22] H. Qin, R. Kumar, and R. Alléaume, "Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 94, Jul. 2016, Art. no. 012325.
[23] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 87, Jun. 2013, Art. no. 062313.
[24] I. Derkach, V. C. Usenko, and R. Filip, "Continuous-variable quantum key distribution with a leakage from state preparation," *Phys. Rev. A, Gen. Phys.*, vol. 96, Dec. 2017, Art. no. 062309.
[25] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, "High-rate measurement-device-independent quantum cryptography," *Nature Photon.*, vol. 9, no. 6, pp. 397–402, Jun. 2015.
[26] 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, Gen. Phys.*, vol. 91, Feb. 2015, Art. no. 022320.
[27] 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, Gen. Phys.*, vol. 89, Apr. 2014, Art. no. 042335.
[28] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, "Continuous-variable measurement-device-independent quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 89, no. 5, May 2014, Art. no. 052301.
[29] H.-X. Ma, P. Huang, D.-Y. Bai, T. Wang, S.-Y. Wang, W.-S. Bao, and G.-H. Zeng, "Long-distance continuous-variable measurement-device-independent quantum key distribution with discrete modulation," *Phys. Rev. A, Gen. Phys.*, vol. 99, Feb. 2019, Art. no. 022322.
[30] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, Mar. 2012, Art. no. 130503.
[31] S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," *Phys. Rev. Lett.*, vol. 108, Mar. 2012, Art. no. 130502.
[32] Z. Li, Y. Zhang, X. Wang, B. Xu, X. Peng, and H. Guo, "Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 93, Jan. 2016, Art. no. 012310.
[33] Y. Zhao, Y. Zhang, B. Xu, S. Yu, and H. Guo, "Continuous-variable measurement-device-independent quantum key distribution with virtual photon subtraction," *Phys. Rev. A, Gen. Phys.*, vol. 97, Apr. 2018, Art. no. 042328.
[34] M. He, R. Malaney, and J. Green, "Quantum communications via satellite with photon subtraction," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–6.
[35] I. B. Djordjevic, "Optimized-eight-state CV-QKD protocol outperforming Gaussian modulation based protocols," *IEEE Photon. J.*, vol. 11, no. 4, Aug. 2019, Art. no. 4500610.
[36] Y. Tamura, H. Sakuma, K. Morita, M. Suzuki, Y. Yamamoto, K. Shimada, Y. Honma, K. Sohma, T. Fujii, and T. Hasegawa, "The first 0.14-dB/km loss optical fiber and its impact on submarine transmission," *J. Lightw. Technol.*, vol. 36, no. 1, pp. 44–49, Jan. 1, 2018.
[37] I. B. Djordjevic, *Advanced Optical and Wireless Communications Systems*. Cham, Switzerland: Springer, 2017.

IVAN B. DJORDJEVIC received the Ph.D. degree from the Faculty of Electronic Engineering, University of Niš, Yugoslavia, in 1999.

He held appointments at the University of the West of England, the University of Bristol, U.K., Tyco Telecommunications, USA, the National Technical University of Athens, Greece, and State Telecommunication Company, Yugoslavia. He is currently a Professor of electrical and computer engineering and optical sciences with The University of Arizona, the Director of the Optical Communications Systems Laboratory (OCSL) and Quantum Communications (QuCom) Laboratory, and the Co-Director of the Signal Processing and Coding Laboratory. He has authored or coauthored seven books, more than 510 journal and conference publications, and 49 U.S. patents.

Dr. Djordjevic is also an OSA Fellow. He also serves as a Senior Editor/Member of Editorial Board/Associate Editor for the following journals: the *Journal of Optical Communications and Networking* (OSA/IEEE), the *Journal of Optics* (IOP), the IEEE COMMUNICATIONS LETTERS, *Physical Communication* journal (Elsevier), and *Frequenz*.