Adaptive Modulation for Continuous-Variable Quantum Key Distribution With Real Local Oscillators Under Phase Attack

Khaled A. Alaghbari, Konstantin Rumyantsev, Tawfig Eltaif, Osama Elmabrok, and Heng-Siong Lim

***Abstract*—Continuous-variable quantum key distribution (CV-QKD) with a real local oscillator (LO) experiences a phase attack security challenge due to the reference pulses transmitted along with quantum signals over an unsecure quantum channel. In this paper, a phase attack on reference pulses of CV-QKD with a real LO is investigated. The performance of the discrete-modulated (DM) CV-QKD under this attack is analyzed analytically and by simulation, and compared with the Gaussian-modulated (GM) CV-QKD. It is found that such an attack by an eavesdropper's, significantly reduce the transmission distance for the GM based CV-QKD, whereas, the DM based CV-QKD shows a high tolerance to high phase noise. Based on phase attack monitoring, a new adaptive modulation scheme is proposed for CV-QKD to adaptively switch between GM and DM so as to maintain the optimum secret key rate.**

***Index Terms*—CV-QKD, quantum cryptography, phase attack, discrete modulation, adaptive modulation.**

I. Introduction

QUANTUM key distribution (QKD) is one of most promising practical applications of quantum cryptography. Its security is based on the laws of quantum physics [1], [2]. QKD offers a secure method for two distant parties to share a sequence of random secure keys over an insecure quantum channel and an authenticated classical channel. Generally, the QKD can be classified into discrete–variable (DV) and continuous-variable (CV) QKQ protocols. The latter are more efficient, as they have greater secure key rates over access and metro dense wavelength division multiplexed (DWDM) networks [3], [4]. The CV-QKD encodes information by varying the quadrature's amplitudes of the quantized electric field. It uses homodyne or heterodyne detections schemes instead of a single-photon detector to recover the secret key. The CV-QKD has been practically implemented and proven to be unconditionally secure in both collective attacks and coherent attacks [5]–[10]. The GM CV-QKD can achieve a high secret key rate, and it has a good compatibility with the classical and modern communication networks. However, it is limited by the transmission distance due to the low reconciliation efficiency compared to its DM CV-QKD counterpart [11]. Using a phase-shift keying (PSK) technique, CV-QKD enables high-speed gigahertz quantum communication [12]. Two-state, four-state [11], and eight-state [13] protocols are the most common techniques used for DM CV-QKD. The larger the number of states, the better the performance in term of secure key rates (SKR) [14].

In CV-QKD systems, Alice, the sender, can send both the signals and local oscillator pulses over the quantum channel. However, the transmission of the LO pulses brings several limitation and loopholes, such as the LO fluctuation attack [15], calibration attacks [16] or saturation attack [17]. Moreover, sending strong LO pulses would reduce the transmission efficiency. In order to overcome these issues, a local-local oscillator (LLO) or a real LO approach was demonstrated in [18], [19], where Alice has a laser source for signals generation and Bob has his own LO for detection. The main challenge in the real LO is that Bob must compensate efficiently the phase drift between two different lasers in order to perform CV-QKD with a tolerable noise level [20]–[22]. The precise phase information for phase compensation at Bob's side is obtained from the reference pulses which are transmitted together with the quantum signals in a time-multiplexing manner. However, these reference pulses are subject to potential threats from the insecure quantum channel. The eavesdropper can manipulate the reference pulses, e.g., by contaminating them with additional phase noises, to increase the phase compensation error. The imperfection in phase compensation due to Eve's phase attack results in potential loopholes that may compromise the generation of secure key in CV-QKD systems. In [23], Bayesian algorithm is suggested as a method that can be utilized by Eve to estimate the phase drift of the reference pulse generated by CV-QKD based on GM or four-state protocols. In [20], a loopholes strategy that could be performed by Eve's phase attack is proposed for GM

Manuscript received August 24, 2021; accepted August 27, 2021. Date of publication September 1, 2021; date of current version September 20, 2021. This work was supported in part by postdoc fellowship granted by the Institute of Computer Technologies and Information Security, Southern Federal University under Project PD/20-01-KT. *(Corresponding author: Khaled A. Alaghbari.)*

Khaled A. Alaghbari is with the Institute of Computer Technologies and Information Security, Southern Federal University, Taganrog 347900, Russia, and also with the Institute of IR4.0, Universiti Kebangsaan Malaysia, Bangi, Selangor 43600, Malaysia (e-mail: khalidazizxp@yahoo.com).

Konstantin Rumyantsev is with the Institute of Computer Technologies and Information Security, Southern Federal University, Taganrog 347900, Russia (e-mail: rke2004@mail.ru).

Tawfig Eltaif is with the Department of Electrical and Electronics Engineering, Xiamen University Malaysia, Selangor 43900, Malaysia (e-mail: tefosat@ieee.org).

Osama Elmabrok is with the Department of Electrical and Electronic Engineering, University of Benghazi Benghazi 1308, Libya (e-mail: osaelmabrok@gmail.com).

Heng-Siong Lim is with the Faculty of Engineering and Technology, Multimedia University, Melaka 75450, Malaysia (e-mail: hslim@mmu.edu.my).

Digital Object Identifier 10.1109/JPHOT.2021.3109060

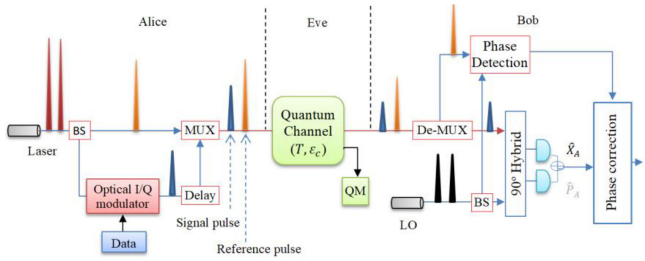

Fig. 1. System model of CV-QKD with a real local oscillator (LO) using homodyne detector.

based CV-QKD, however, to the best of our knowledge, the above-mentioned method has not been studied and evaluated adequately for DM based CV-QKD protocol. In addition, the authors in [20] proposed a method to monitor the deviation of phase compensation error on quantum signals and on reference pulses to discover eavesdropping, so that Alice and Bob can switch the quantum channel to more secure one. In [24], an adaptable transmitter that is able to switch between DV-QKD and CV-QKD is designed for re-configurable optical networks. Inspired by the above works, we propose an adaptive modulation scheme for CV-QKD that switches between GM and DM based on the deviation of phase compensation error. The proposed system can maintain the high optimum secret key rate when the phase noise increases. One important feature of the proposed system is the usage of a single transmitter and single receiver with switching capability in the modulation type of CV-QKD. In contract to [24], a single transmitter with switching capability is used and two independent receivers are required to switch between discrete-variable (DV) and continuous variable (CV) QKD. The new adaptive modulation CV-QKD could find application in the context of agile and versatile quantum cryptography, where the same hardware could be used for dynamically switching modulation schemes according to the prevailing phase attack in order to achieve the optimum secret key rate. The rest of this paper is organized as follows: Section 2 presents CV-QKD system model with a real LO that can be used for DM or GM input data. It is then followed by describing the phase errors compensation and phase attack method by Eve. Section 3 demonstrates the security analysis of CV-QKD protocol under phase attack. Section 4 presents our simulation findings for the secret key rates and phase attack detection. Finally, conclusion is drawn in section 5.

II. System Model

The CV-QKD system with a real local oscillator (LO) is illustrated in Fig. 1. The sender, Alice, employs a laser source to generate a set of optical pulses that are separated by beam splitter (BS) into signal and reference paths. In the former, quantum signals of Gaussian-modulated (GM) or discrete-modulated (DM) coherent states $|X_A + iP_A\rangle$ are generated. This is obtained from two independent random variables with zero-mean and modulation variance V_A (see Appendix A for more details about the generation of two-state, four-state and eight-state). The optical pulses are then modulated by in-phase quadrature (IQ) optical modulator. The quantum signals are delayed and multiplexed with reference pulses in time-domain and sent to Bob over a quantum channel. The channel is characterized by transmittance T and excess noise ε_c. The latter is due Eve activities and imperfect phase compensation error (PCE) $\delta\varphi_s'$, which causes a random phase rotation between Alice's modulated coherent state (X_A, P_A) and Bob's measured state (X_B, P_B). Consequently, the quantum state received at Bob's side can be written as [20]–[22]:

$$X_B = \sqrt{T}\left(X_A \cos\delta\varphi_s^{'} - P_A \sin\delta\varphi_s^{'}\right) + X_N \quad (1)$$

$$P_B = \sqrt{T}\left(X_A \sin\delta\varphi_s^{'} - P_A \cos\delta\varphi_s^{'}\right) + P_N, \quad (2)$$

where X_N and P_N are random Gaussian noises with variance $T\varepsilon_c$ for quadrature X_B and P_B, respectively. The total channel-added noise is given, in shot noise units (SNU), as $\chi_{line} = 1/T - 1 + \varepsilon_c$. Since the transmission over the quantum channel induces a phase rotation on the quantum signal, a strong reference pulse with quadrature X_A^R and P_A^R is transmitted along each quantum pulse to recover the initial phase of the quantum signal.

At the receiver Bob's side, the incoming pulses are demultiplexed and split into quantum path and reference path. The reference pulses with quadratures X_B^R and P_B^R , which are assumed to experience the same distortion as described in (1) and (2), are measured by Bob to estimate the phase drifts between Alice's laser and Bob's LO. This is done by using:

$$\delta\,\hat{\varphi}_R' = \tan^{-1}\left(X_B^R/P_B^R\right) \quad (3)$$

and this to be used later to compensate the phase error for the quantum signals. A homodyne detector or heterodyne detector is used by Bob to measure either one (or both) of amplitude quadrature $\hat{X}_A$ and phase quadrature $\hat{P}_A$ of the received quantum pulses. In this paper, a homodyne detector is considered. The phases of measured quantum signals are then compensated by the estimated reference pulses phases. In practical detector with detection efficiency η and electronic noise v_{el} in SNU, the detection-added noise referred to Bob's input is expressed by $\chi_{hom} = (1 + v_{el})/\eta - 1$ for homodyne detector and the total noise referred to the channel input is expressed by $\chi_{tot} = \chi_{line} + \chi_{\text{hom}}/T$ [20], [22].

A. Phase Compensation

For the quantum signals, the relative phase drift caused by Alice' laser and Bob's LO is given by [20]:

$$\emptyset_s = \theta_A - \theta_B + \varphi_s^{ch} \quad (4)$$

where θ_A and θ_B are phases of the quantum pulse from Alice's laser and Bob's LO respectively, and φ_s^{ch} is phase drift caused by the quantum channel. Similarly, the relative phase drift induced to the reference pulse is given by:

$$\emptyset_R = \theta_A - \theta_B + \varphi_R^{ch} \quad (5)$$

In (5), φ_R^{ch} is the relative phase drift of the reference pulse due to the quantum channel. If we assume that the phase jitter of Alice's laser and Bob's LO are negligible, then the relative

phase drift of the quantum signal can be estimated by that of the reference pulse. Thus, the phase compensation error (PCE) on the quantum signal is given by:

$$\delta\, \emptyset_s = \emptyset_s \; - \; \emptyset_R = \varphi_s^{ch} - \varphi_R^{ch} \tag{6}$$

B. Eve's Phase Attack

The purpose of the reference pulses is to provide precise phase information for phase compensation on Bob's side, but these reference pulses are also vulnerable to threats from the insecure quantum channel. If eavesdroppers manipulate these reference pulses, the phase information carried by them becomes unreliable, and the phase compensation for coherent detection becomes imperfect. The imperfect phase compensation reduces the security of the CVQKD scheme [20], [23].

As a result of Eve's phase attack, the relative phase drifts of reference pulses are interfered by additional phase noise, which is given by [20]

$$\emptyset'_R = \emptyset_R + \varphi_R^{attack} \tag{7}$$

where φ_R^{attack} is the additional phase noise caused by Eve's phase attack on the reference pulse. This would increase the PCE and yield imperfect phase compensation. Therefore the actual PCE of the quantum signal needs to be re-written as [20]:

$$\delta\, \emptyset'_s = \varphi_s^{ch} - \varphi_R^{ch} \; - \varphi_R^{attack} \tag{8}$$

and the deviation of the actual PCE is then written as:

$$V_s = V_s^{ch} \; + V_R^{ch} + \; V_R^{attack} = 2V_{ch} \; + V_{attack} \tag{9}$$

where the phase noise of the quantum channel is assumed to be zero-mean with variance of V_{ch} for the quantum pulses, and also for the reference pulses since they are transmitted over the same channel. The phase noise caused by Eve' attack is assumed to be zero-mean with variance V_{attack}.

C. Phase Attack Detection

The phase noise created by Eve's attack is mixed up with that of the quantum channel, making it difficult to be distinguished from the actual PCE. The deviation of PCE on both the quantum and the reference pulses signals can be monitored in real-time by Bob [20]. This is accomplished by randomly choosing *M* quantum signals as training signals from *N* blocks of the incoming quantum signals.

The actual PCE of the reference pulses can be monitored and estimated from the phase of the current reference pulse (*i*) and next reference pulse (*i*+1) as [20]:

$$\delta\, \emptyset'_{R,i} = \emptyset'_{R,i} \; - \emptyset'_{R,i+1} \tag{10}$$

and the deviation of PCE on the reference pulses is given by:

$$\begin{aligned} V_R &= \left(V_{R,i}^{ch} + V_{R,i}^{attack}\right) \; + \left(V_{R,i+1}^{ch} + V_{R,i+1}^{attack}\right) \\ &= 2V_{ch} + 2V_{attack} \end{aligned} \tag{11}$$

In (10), the phase noise caused by Eve's attack on two successive reference pulses (*i* and *i*+1) are assumed to be constant during the transmission. If there is a phase attack by Eve, the deviation of PCE on the reference pulses will differ from that on the quantum signals, allowing the phase attack to be detected. This phenomenon can be exploited for measuring the intensity of phase attack, so that the participants can determine whether or not phase attack is present. Moreover, the difference of the deviation of PCE between the reference pulses and quantum signals can be utilized by the two remote participants for adapting the transmission modulation to improve security.

After estimating the phase of the reference pulses using (3), the phase of current quantum signal (*i*) is estimated using the average value of current (*i*) and next (*i*+1) reference pulses phases as [18]:

$$\delta\hat{\varphi}'_s \;(i) = \; \frac{1}{2}\left(\delta\varphi'_R\,(i+1) + \delta\varphi'_R\,(i)\right) \tag{12}$$

Using this estimated phase information, Bob can recover his measurement results for quantum signal by executing the following rotation process:

$$\hat{X}_A = \left(X_B \cos\delta\hat{\varphi}'_s + P_B \sin\delta\hat{\varphi}'_s\right) \tag{13}$$

$$\hat{P}_A = \left(-X_B \sin\delta\hat{\varphi}'_s + P_B \cos\delta\hat{\varphi}'_s\right) \tag{14}$$

D. Security Analysis With Phase Attack

The noise model of imperfect phase compensation for the traditional GM CV-QKD [18]–[23] is used in this paper to evaluate the practical security of the CV-QKD with real LOs. The actual phase compensation error $\delta\varphi'_s$ is assumed to be zero-mean in the noise model of imperfect phase compensation. In this case, the covariance matrix of the mixture state ρ_{AB} exchanged via Alice and Bob can be expressed by:

$$\gamma_{AB} = \begin{pmatrix} \gamma_A & \sigma_{AB} \\ \sigma_{AB} & \gamma_B \end{pmatrix} \; = \begin{pmatrix} V\mathbf{I}_2 & \sqrt{T_\kappa}Z\sigma_z \\ \sqrt{T_\kappa}Z\sigma_z & T_K\left(V + \chi_{tot}^{\kappa}\right)\mathbf{I}_2 \end{pmatrix} \tag{15}$$

where $\mathbf{I}_2$ is a second-order identity matrix, $\sigma_z = \; \mathrm{diag}(1, -1)$, the correlation coefficient *Z* for GM, two-state, four-state and eight-state based CV-QKD are given respectively as [11], [13]:

$$\begin{aligned} Z_G &= \sqrt{(V^2 - 1)}, \\ Z_2 &= 2\alpha^2\left(\lambda_0^{3/2}\lambda_1^{-1/2} + \lambda_1^{3/2}\lambda_0^{-1/2}\right), \\ Z_4 &= 2\alpha^2 \sum_{k\,=\,0}^{3}\left(\lambda_{k-1}^{3/2}\lambda_k^{-1/2}\right), \\ \text{and } \; Z_8 &= 2\alpha^2 \sum_{k\,=\,0}^{7}\left(\lambda_{k-1}^{3/2}\lambda_k^{-1/2}\right), \end{aligned} \tag{16}$$

where λ is as defined in Appendix A for each corresponding protocols. $V \; = V_A \; + 1$, and V_A is Alice's modulation variance. The term T_κ represents the actual transmittance, and the term χ_{tot}^{κ} represents the actual total noise referred to the channel input. In addition, the actual transmittance due to the imperfect phase compensation can be written as [20], [24]:

$$T_\kappa = \; \kappa T, \tag{17}$$

where κ represents the phase compensation accuracy. The actual total noise can be expressed as:

$$\chi_{tot}^{\kappa} = \chi_{\text{line}}^{\kappa} + \chi_{\text{hom}}/T_{\kappa}, \tag{18}$$

where $\chi_{\text{line}}^{\kappa} = 1/T_{\kappa} + \varepsilon_c^{\kappa}$ represents the actual total channel-added noise referred to the channel input, and ε_c^{κ} characterizes the actual excess noise given by:

$$\varepsilon_c^{\kappa} = \left[\varepsilon_c + (1-\kappa)(V-1)\right]/\kappa. \tag{19}$$

For imperfect phase compensation in CV-QKD, the terms T_{κ} and ε_c^{κ} are closely associated to the accuracy of phase compensation term κ as:

$$\kappa = \left(E\left[\cos\delta\varphi_s'\right]\right)^2 \tag{20}$$

where $E[\cdot]$ represents the expectation. As long as the actual phase compensation error $\delta\varphi_s'$ is smaller than 5 degrees, the Taylor series approximation $\cos x = 1 - x^2/2$ can be realized; hence the accuracy of phase compensation can be estimated as [20], [24]:

$$\kappa' = \left(1 - \frac{1}{2}V_s\right)^2 \tag{21}$$

where V_s is the deviation of phase compensation error given by (9).

For the case of reverse reconciliation under collective attack, the secret key rate of the CV-QKD system is calculated asymptotically as [5], [26]:

$$K = \beta I_{AB} - \chi_{BE} \tag{22}$$

where $\beta \in (01)$ is the reverse reconciliation efficiency, I_{AB} is the Shannon mutual information of Alice and Bob, and χ_{BE} is the Holevo bound that defines the maximum information available to Eve on Bob's secret information. The mutual information I_{AB} is derived from Bob's measured variance V_B and the conditional variance $V_{B|A}$ using Shannon's equation of homodyne detection that is employed by Bob:

$$I_{AB} = \frac{1}{2}\log_2\frac{V_B}{V_{B|A}} = \frac{1}{2}\log_2\frac{V+\chi_{tot}^{\kappa}}{1+\chi_{tot}^{\kappa}} \tag{23}$$

where V_B is Bob's variance and $V_{B|A}$ is the conditional variance of Alice based on Bob's measurement. The mutual information I_{AB} for heterodyne detection is double of that in (22). The Holevo bound can be calculated from the covariance matrix γ_{AB} presented in Eq. (15) and then it can be derived as [5]:

$$\chi_{BE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right) \tag{24}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, and the symplectic eigenvalues $\lambda_i (i = 12, \ldots, 5)$ are given by

$$\lambda_{12}^2 = \frac{1}{2}\left(A \pm \sqrt{A^2 - 4B}\right) \tag{25}$$

$$\lambda_{34}^2 = \frac{1}{2}\left(C \pm \sqrt{C^2 - 4D}\right) \tag{26}$$

and $\lambda_5 = 1$ with

$$A = V^2 + 2T_{\kappa}\left(1 - V^2\right) + T_{\kappa}^2\left(V + \chi_{\text{line}}^{\kappa}\right)^2 \tag{27}$$

$$B = \det\gamma_{AB} = T_{\kappa}^2\left(1 + V\chi_{\text{line}}^{\kappa}\right)^2 \tag{28}$$

$$C = \frac{A\chi_{hom} + V\sqrt{B} + T_{\kappa}\left(V + \chi_{\text{line}}^{\kappa}\right)}{T_{\kappa}\left(V + \chi_{\text{line}}^{\kappa}\right)} \tag{29}$$

$$\text{and } D = \frac{V\sqrt{B} + B\chi_{hom}}{T_{\kappa}\left(V + \chi_{\text{line}}^{\kappa}\right)} \tag{30}$$

E. Estimation of Transmittance and Excess Noise Parameters

The estimation of the transmittance T_{κ} and excess noise ε_c^{κ} can be accomplished by using training signal of length *M* that are randomly selected from Bob's received quantum signals such that:

$$\hat{T}_{\kappa} = \left|\frac{yx^H}{xx^H}\right|^2 \tag{31}$$

and

$$\hat{\varepsilon}_c^{\kappa} = \frac{1}{M\hat{T}_{\kappa}}\left[\left(y - \sqrt{\hat{T}_{\kappa}}x\right)\left(y - \sqrt{\hat{T}_{\kappa}}x\right)^H\right] \tag{32}$$

where $(\cdot)^H$ is conjugate-transpose operator, $|\cdot|$ is absolute value operator, x is the modulated quadrature of the training signal announced by Alice by a classical channel, and y is the quadrature measurement at Bob's side.

III. Result and Discussion

In this section, we present simulation and analytical evaluations of the CV-QKD under phase attack. We compare between different CV-QKD protocols such as Gaussian modulation (GM) protocol and discrete modulation (DV) protocols with 2-state, 4-state and 8-state. The following parameters are assumed as determined by previous practical CV-QKD experiment: electronic noise $v_{el} = 0.001$, excess noise $\varepsilon_c = 0.01$ (in shot noise units, SNU) for all protocols except 2-state which has $\varepsilon_c = 0.001$, reconciliation efficiency $\beta = 0.926$ and detection efficiency $\eta = 0.59$. We assume the channel between Alice and Bob is optical fiber with 0.2 dB/km attenuation coefficient, and the channel transmittance is expressed as $T = 10^{-0.2L/10}$, where *L* is the fiber length in kilometers. In the simulation, 5000 Gaussian-modulated (or discrete-modulated) quantum states are generated for GM protocols (or DM protocols) [20]. The signal is then contaminated by normally-distributed phase noise and transmitted over a channel characterized by transmittance *T* and excess noise ε_c as described in (1) and (2). The theoretical curves are plotted using the actual values of transmittance T_{κ} and excess noise ε_c^{κ}, on the other hand, the simulated curves are plotted based on the estimated values of $\hat{T}_{\kappa}$ and $\hat{\varepsilon}_c^{\kappa}$ as described in (31) and (32). The simulation results are used to confirm the validity of the theoretical results and also to approximate the practical secret key rate (SKR).

Fig. 2 shows the secret key rate (SKR) that can be achieved by GM, 2-state, 4-state and 8-state protocols without phase attack. The modulation variances are optimized with 4, 0.035, 0.35 and 0.35 for GM, 2-state, 4-state and 8-state protocols respectively. The GM provides the best SKR followed by 8-state which achieves slightly better SKR than the 4-state. Some experimental

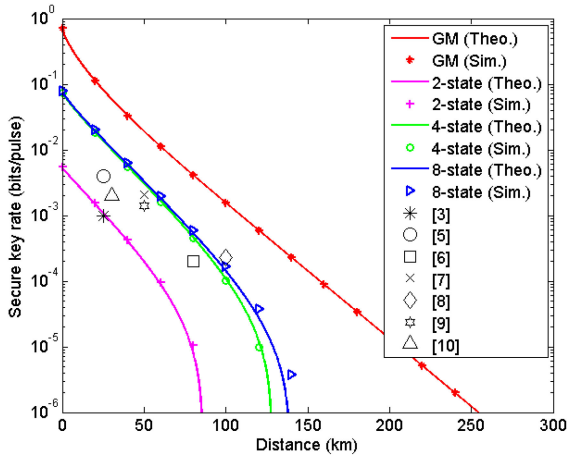

Fig. 2. Theoretical and simulated secret key rates as a function of transmission distance. GM with modulation variance of 4, 2-state with modulation variance of 0.035, and 4-state and 8-state with modulation variance of 0.35.The phase attack is zero, and excess noise is $\varepsilon_c = 0.01$ for all protocols except for 2-state protocol, where $\varepsilon_c = 0.001$.

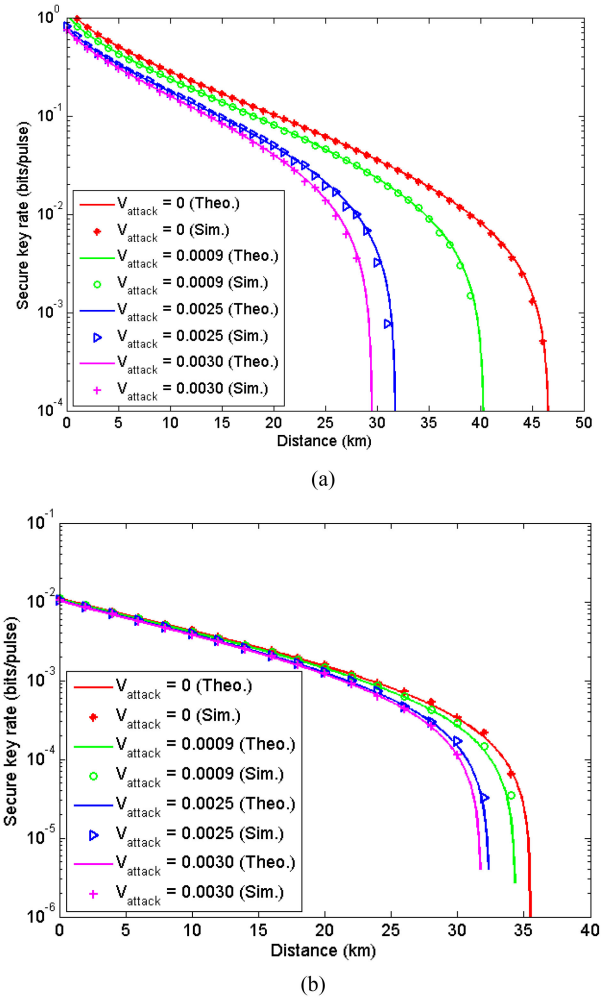

Fig. 3. The theoretical and simulated secret key rates under phase attack as function of transmission distance for (a) GM-based CV-QKD with $V_A = 18.9$ (b) 4-state based CV-QKD with $V_A = 0.1$.

results presented in [3], [5]–[9] for GM and [10] for four-state protocols are plotted for comparison. For example, in [3] and [5], SKRs of about 100 k bit/second and 2k bits/second are achieved at distance a of 25km using pulse rates of 100 MHz and 500 kHz respectively; in [7] and [9], SKRs of 52 k and 700 bits/second are achieved at 50km with pulse rates of 25 MHz and 500 kHz respectively. Experiments in [6] and [8] achieved secret key rates of about 200 and 450 bits/second at distances of 80 km and 100 km using pulse rates of 1 MHz and 2 MHz respectively. In [10], the authors implemented a 4-state protocol and achieved a SKR of 1k bits/second at distance of 30.2 km using pulse rate of 500 kHz. We can see that the achieved transmission distance by the experiments above are less than 100 km, even though, the theoretical maximum transmission can (asymptotically) reach up to 250 km with SKR of 10^{-6} for GM, 127 km for 4-state and 138 km for 8-state. The SKR achieved by the experimental GM based CV-QKD is close to that of the theoretical 4-state and 8-state protocols. The gap between the experimental and theoretical results is due to additional factors such as the accuracy of phase noise estimation, reconciliation efficiency, excess noise fluctuation and modulation variance adjustment.

Fig. 3 shows the secret key rates for the GM based CVQKD (Fig. 3(a)) and four-state (Fig. 3(b)) systems under different phase attacks versus the transmission distance. We set the modulation variance of GM to 18.9 based on the experiment in [23], and 0.1 for 4-state. We assumed the phase noise of quantum channel is normally distributed with variance $V_{ch} = 0.0001$ rad^2, and that of Eve's phase attack is normally distributed with variance $V_{attack} = 0,\ 0.0009,\ 0.0025$ and 0.0030 (rad^2). In addition, the theoretical secret key rates of the CV-QKD system under phase attack and based on the noise model of imperfect phase compensation are evaluated and plotted in Fig. 3 for comparison purpose. Fig. 3(a) shows that, increasing the phase noise variance due to Eve' attack degrades significantly the transmission distance and the secret key rate of the GM-based system. However, the four-state system is relatively less affected by the phase noise variance as illustrated in Fig. 3(b).

In Fig. 4, we evaluated the security of CV-QKD under phase attack as a function of the modulation variance V_A. The modulation variance can be optimized to improve the system performance as suggested in Fig. 4(a). While the GM protocol under only quantum channel phase noise ($V_{attack} = 0$) , would allow large possible values of V_A. The values of V_A is restricted to certain range when the there is a phase attack by Eve. On the other hand, the four-state protocol shows robustness to the changes in the phase attack. Fig. 4(b) presents the optimum V_A that is reduced as the transmission distance increases and reached to about 4 for GM protocol, which should give us the maximum achievable performance when the transmission distance is greater than 40km. However, the optimum V_A for four-state protocols keeps decreasing as the transmission distance increases.

Fig. 5 illustrates the theoretical and simulation results of phase attack detection for 4-state based CV-QKD with $V_A = 0.5$, where the phase noise of quantum channel is assumed to be

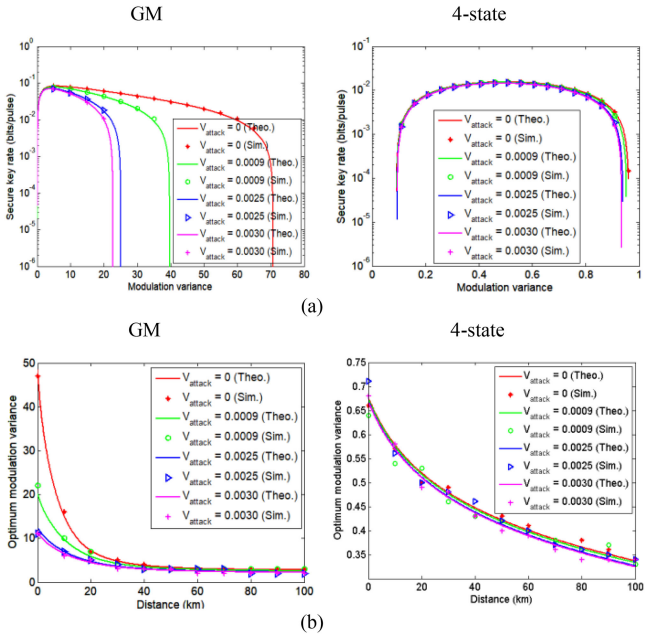

Fig. 4. (a) Theoretical and simulated secret key rates as function of modulation variance at transmission distance of 25km (b) Optimum modulation variance over transmission distance, for GM and four-state protocols.

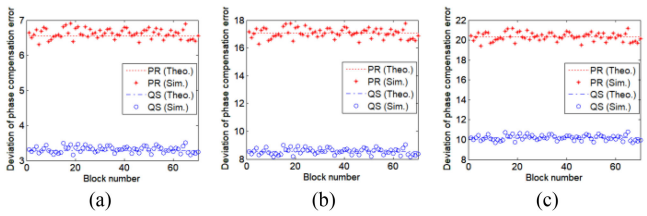

Fig. 5. The deviation of phase compensation error with respect to quantum signals (QS) and reference pulses (RP) of 4-state CV-QKD with $V_A = 0.5$ and $\varepsilon_c = 0.01$ at 25km. The phase noise variance of quantum channel is 0.0001, while Eve's attack causes phase noise variance of (a) 0.0009 (b) 0.0025 (c) 0.0030, the theoretical deviations are represented by dash line while the deviations estimated by reference signals are represented by circles and crosses markers.

TABLE I
THEORETICAL DEVIATION OF PHASE COMPENSATION ERROR ON QS AND RP

V_{attack}	0.0009	0.0025	0.0030
Quantum signal (QS)	0.0010 (rad^2) 3.28 (degree^2)	0.0026 (rad^2) 8.53 (degree^2)	0.0031 (rad^2) 10.18(degree^2)
Reference pulses (RP)	0.0020 (rad^2) 6.56 (degree^2)	0.0052 (rad^2) 17.07 (degree^2)	0.0062 (rad^2) 20.35 (degree^2)

normally distributed with variance $V_{ch} = 0.0001$ (rad^2) and phase noise that is caused by Eve's attack is set to $V_{attack} = 0.0009,\ 0.0025$ and 0.0030. The deviation of phase compensation error on the quantum signal and on the reference pulses (RP) can be calculated theoretically using Eq. (9) and (11) respectively as shown in Table I. In the simulation, we assumed the quantum signals (QS) are affected by phase noise of quantum channel and by Eve's phase attack simultaneously. A reference signal of length 5000 and variance of 200 is used to estimate the phase compensation error on the quantum signals using (3) and (12). Then the deviation of PCE on the reference pulse is estimated using the variance of (3), and the deviation of PCE

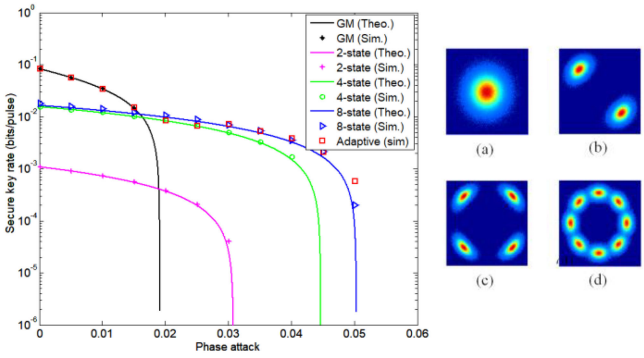

Fig. 6. Theoretical and simulated secret key rate as function of phase noise caused by Eve's attack with constellation diagram for (a) GM, (b) 2-state, (c) 4-state and (d) 8-state at phase attack noise of 0.015, excess noise is $\varepsilon_c = 0.01$ except for 2-state with $\varepsilon_c = 0.001$.

on the quantum signal is estimated using the variance of (12). Fig. 5 shows very close agreement between the theoretical and simulated results over a block of 70, which depends on the variance of reference signal and excess noise. It can also be observed, when the phase attack is more severe, the difference of the deviation of PCE between the quantum signal and reference signal will increase. For example, when Eve's attack is $V_{attack} = 0.0009,\ 0.0025$ and 0.0030, the difference of deviation of PCE between the QS and RP are 3.28, 8.53 and 10.17 respectively. This can be exploited to help Alice and Bob evaluate the strength of Eve's phase attack, and a new adaptive modulation scheme for CV-QKD can be developed to switch between different modulations in order to keep the SKR as high as possible.

We next evaluate the SKR of the four protocols versus different phase noise that is caused by Eve's attack. The modulation variance is optimized at 25 km so that GM, 2-state, 4-state and 8-state have 6, 0.035, 0.5 and 0.5 in SNU respectively. Fig. 6 also shows the constellation diagrams of the four modulations with phase attack of 0.015. The GM provides high SKR up to phase noise level of 0.157 then it starts to degrade rapidly. The discrete-modulated based CV-QKD, especially the 8-state provides high tolerance against the phase attack compared to GM. The proposed adaptive CV-QKD is designed to switch from GM to 4-state protocol when the difference in the deviation of PCE for the reference pulses and quantum signals exceeds 40, and to switch from 4-state to 8-state protocol when the difference is greater than 80. The proposed technique is able to maintain the optimum secret key rate even for very high phase noise. The proposed system could increase the system overhead because it requires the transmitter to know the current state of the phase attack so that the best modulation scheme can be chosen. In addition, the receiver must be informed of the selected modulation scheme in order to decode the information correctly.

IV. CONCLUSION

In this paper, we have analysed the security performance of CV-QKD with local oscillator under phase attack by Eve. We found that the discrete-modulated based CV-QKD has

good robustness against the phase noise compared to Gaussian-modulated (GM) CV-QKD. The findings also show that the theoretical secret key rate (SKR) matches the simulated SKR which is estimated using training signals. Moreover, a strategy to detect the severity of phase attack by Eve is tested for CV-QKD, by monitoring the phase compensation error on the quantum signal and reference pulses in real-time. It is then effectively exploited to design a new adaptive modulation scheme for CV-QKD that is capable of switching between different modulations to achieve the highest possible SKR.

APPENDIX A

For discrete modulation CV-QKD, Alice send n random coherent state with 1/2, 1/4 and 1/8 probability drawn from two-state S_2, four-state S_4 or eight-state S_8 respectively as:

$$S_2 = |\alpha e^{-i\pi/4}\rangle \text{ and } |-\alpha e^{-i\pi/4}\rangle,$$

$$S_4 = |\alpha e^{i\pi/4}\rangle,$$

$|\alpha e^{i3\pi/4}\rangle$,$|\alpha e^{i5\pi/4}\rangle$ and $|\alpha e^{i7\pi/4}\rangle$,

$$S_8 = |\alpha\rangle,$$

$|\alpha e^{i\pi/4}\rangle$,$|\alpha e^{i\pi/2}\rangle$,$|\alpha e^{i3\pi/4}\rangle$,$|\alpha e^{i\pi}\rangle$,$|\alpha e^{i5\pi/4}\rangle$,$|\alpha e^{i3\pi/2}\rangle$ and $|\alpha e^{i7\pi/4}\rangle$where α is a real positive number related to modulation variance V_A such as $V_A = 2\alpha^2$.

The generated coherent state is sent over quantum channel to Bob. Bob then obtains a mixture state with density matrix ρ. For 2-state system, the density matrix is given by: $\rho_2 = \lambda_0 \ |\phi_0\rangle\langle\phi_0| + \lambda_1|\phi_1\rangle\langle\phi_1|$ where $\lambda_0 = e^{-\alpha^2} \ \cosh\alpha^2$, $\lambda_1 = e^{-\alpha^2} \ \sinh\alpha^2$.

For 4-state, the density matrix is given by: $\rho_4 = \sum_{i=0}^{3} \lambda_i \ |\phi_i\rangle\langle\phi_i|$, where $\lambda_{02} = \frac{1}{2}e^{-\alpha^2}\ (\cosh\alpha^2 \pm \cos\alpha^2)$, and $\lambda_{13} = \frac{1}{2}\ e^{-\alpha^2}(\sinh\alpha^2 \pm \sin\alpha^2)$.

For 8-state, the density matrix is given by: $\rho_8 = \sum_{i=0}^{7} \lambda_i \ |\phi_i\rangle\langle\phi_i|$ with

$$\lambda_{04} = \frac{1}{4}e^{-\alpha^2}\ \left(\cosh\alpha^2 + \cos\alpha^2 \pm 2\cos\frac{\alpha^2}{\sqrt{2}}\cosh\frac{\alpha^2}{\sqrt{2}}\right),$$

$$\lambda_{15} = \frac{1}{4}e^{-\alpha^2}\ \left(\sinh\alpha^2 + \sin\alpha^2 \pm \sqrt{2}\cos\frac{\alpha^2}{\sqrt{2}}\sinh\frac{\alpha^2}{\sqrt{2}} \pm\sqrt{2}\sin\frac{\alpha^2}{\sqrt{2}}\cosh\frac{\alpha^2}{\sqrt{2}}\right),$$

$$\lambda_{26} = \frac{1}{4}e^{-\alpha^2}\ \left(\cosh\alpha^2 - \cos\alpha^2 \pm 2\sin\frac{\alpha^2}{\sqrt{2}}\sinh\frac{\alpha^2}{\sqrt{2}}\right),$$

$$\lambda_{37} = \frac{1}{4}e^{-\alpha^2}\ \left(\sinh\alpha^2 - \sin\alpha^2 \mp \sqrt{2}\cos\frac{\alpha^2}{\sqrt{2}}\sinh\frac{\alpha^2}{\sqrt{2}} \pm\sqrt{2}\sin\frac{\alpha^2}{\sqrt{2}}\cosh\frac{\alpha^2}{\sqrt{2}}\right).$$

REFERENCES

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

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

[3] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, "High-speed continuous-variable quantum key distribution without sending a local oscillator," *Opt. Lett.*, vol. 40, pp. 3695–3698, 2015.

[4] Y.-M. Chi *et al.*, "A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution," *New J. Phys.*, vol. 13, pp. 1–8, 2011.

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

[6] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nat. Photon.*, vol. 7, pp. 378–381, 2013.

[7] C. Wang, D. Huang, P. Huang, D. Lin, J. Peng, and G. Zeng, "25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel," *Sci. Rep.*, vol. 5, 2015, Art. no. 14607.

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

[9] X. Y. Wang, W. Y. Liu, P. Wang, and Y. M. Li, "Experimental study on all-fiber-based unidimensional continuous variable quantum key distribution," *Phys. Rev. A*, vol. 95, no. 6, 2017, Art. no. 062330.

[10] X. Y. Wang, Z. L. Bai, S. F. Wang, Y. M. Li, and K. C. Peng, "Four-state modulation continuous variable quantum key distribution over a 30-km fiber and analysis of excess noise," *Chin. Phys. Lett.*, vol. 30, no. 1, 2013, Art. no. 010305.

[11] 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.

[12] 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, 2016.

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

[14] X. Wang, S. Guo, P. Wang, W. Liu, and Y. Li, "Realistic rate–distance limit of continuous-variable quantum key distribution," *Opt. Exp.*, vol. 27, pp. 13372–13386, 2019.

[15] X. Ma, S. Sun, M. Jiang, and L. Liang, "Local oscillator fluctuation opens a loophole for eve in practical continuous-variable quantum key-distribution systems," *Phys. Rev. A*, vol. 88, 2013, Art. no. 022339.

[16] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 87, 2013, Art. no. 062313.

[17] H. Qin, R. Kumar, and R. Alléaume, "Saturation attack on continuous-variable quantum key distribution system," in *Proc. SPIE* 8899, 88990N 2013, pp. 1–7.

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

[19] D. B. S. Soh *et al.*, "Self-referenced continuous-variable quantum key distribution protocol," *Phys. Rev. X*, vol. 5, 2015, Art. no. 041010.

[20] B. Huang, Y. Huang, and Z. Peng, "Practical security of the continuous-variable quantum key distribution with real local oscillators under phase attack," *Opt. Exp.*, vol. 27, pp. 20621–20631, 2019.

[21] A. Marie and R. Alleaume, "Self-coherent phase reference sharing for continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 95, no. 1, pp. 01231–01246, 2017.

[22] S. Ren, R. Kumar, A. Wonfor, X. Tang, R. Penty, and I. White, "Reference pulse attack on continuous variable quantum key distribution with local local oscillator under trusted phase noise," *J. Opt. Soc. Amer. B*, vol. 36, no. 3, pp. B7–B15, 2019.

[23] W. Zhao, R. Shi, and D. Huang, "Practical security analysis of reference pulses for continuous-variable quantum key distribution," *Sci. Rep.*, vol. 9, 2019, Art. no. 18155.

[24] I. H. Lopez Grande, S. Etcheverry, J. Aldama, S. Ghasemi, D. Nolan, and V. Pruneri, "Adaptable transmitter for discrete and continuous variable quantum key distribution," *Opt. Exp.*, vol. 29, pp. 14815–14827, 2021.

[25] P. Huang, D. Lin, D. Huang, and G. Zeng, "Security of continuous-variable quantum key distribution with imperfect phase compensation," *Int. J. Theor. Phys.*, vol. 54, no. 8, pp. 2613–2622, 2015.

[26] 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*, vol. 42, 2009, Art. no. 114014.