



Deposited via The University of York.

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/id/eprint/200173/>

Version: Other

Preprint:

Ren, Shengjun, Kumar, Rupesh, Wonfor, Adrian et al. (2017) Reference Pulse Attack on Continuous-Variable Quantum Key Distribution with Local Local Oscillator. [Preprint]

Reuse

Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

Reference Pulse Attack on Continuous-Variable Quantum Key Distribution with Local Local Oscillator

Shengjun Ren^{1,*}, Rupesh Kumar², Adrian Wonfor¹, Xinke Tang¹, Richard Pentyl¹, and Ian White¹

¹*Centre for photonic systems, University of Cambridge, UK, CB3 0FA*

²*Quantum Communication Hub, University of York, UK, YO10 5DD*

We reveal a security loophole in the current state-of-art phase reference pulse sharing scheme for Continuous Variable Quantum Key Distribution using a Local Local Oscillator (LLO-CVQKD). The loophole is associated with the amplitude of the phase reference pulses which Eve can manipulate to extract excess information which cannot be discovered by legitimate users. We call this new attack as the ‘reference pulse attack’. We have demonstrated the efficiency of our attack for different LLO-CVQKD transmission distances. Unity attack efficiency can be achieved at a transmission distance greater than 21.2 km in the case of a zero loss channel. The distance extends to 24.3 km where hollow-core fibre channels are used. We also propose possible countermeasures.

I. Introduction:

The aim of quantum key distribution (QKD) is to promise information security between two authenticated users (Alice and Bob), connected by a classical channel and a quantum channel. This is achieved by sharing common random encryption codes which are unknown to the eavesdropper, Eve [1][2][3][4]. Continuous Variable (CV) QKD technology has rapidly developed in the recent years [5][6][7] and its protocols take advantage of the properties of light associated with waves, such as amplitude and phase, and encrypt keys in quadrature of the electromagnetic field which can be extracted with coherent detection techniques. The primary advantage of CVQKD is its compatibility with standard off-the-shelf optical communication components which could enable more affordable QKD networks [8]. In addition, compared with dedicated single-photon detector based discrete variable (DV) QKD systems, coherent detection allows CVQKD systems to have much higher potential key rates at short distance[9][10][11]. Furthermore, single optical integrated circuits are feasible [12] allowing CVQKD devices to be integrated with classical dense wavelength division multiplexing components [13]. A number of CVQKD protocols exist, but Gaussian-modulated coherent-state (GMCS) CVQKD having been rigorously studied and shown to provide unconditional security against malicious eavesdropping [14][15][16]. However, imperfections in real CVQKD systems result in potential loopholes that compromise the secure key generation. For example, attacks that exploit the intensity fluctuations of

the local oscillator (LO) [17], the wavelength dependency of homodyne beam splitter [18], and the saturation of homodyne detector [19], have been identified and respective counter measures have been proposed.

The Local Local Oscillator (LLO) CVQKD system, proposed and demonstrated in [20][21][22], obviates the need for direct transmission of a LO from Alice to Bob and thereby nullifies the scope for direct or indirect attacks on the LO. This is achieved by using independent narrow linewidth lasers of the same wavelength, one at Alice for signal generation and the other at Bob for local oscillator use. This scheme also facilitates the coexistence of CVQKD systems with classical coherent detection at high repetition rate [22]. However, agreeing a common phase reference between the two free running lasers is an experimental challenge. In order to ease such a limitation, Alice can share low intense phase reference pulses with Bob, and he can correct the LO laser phase in real time [23] or otherwise can adjust the measured quadrature outcomes later during data reconciliation [24]. Due to the relatively small signal magnitude, the quantum uncertainty associated with the phase of the reference pulse induces a phase estimation error in Bob’s quadrature measurement and this amplitude-related noise can result in a loophole for Eve to mount an attack. This loophole has not been investigated in the security analysis of the LLO-CVQKD system to date and as a result, estimations of the derived secret key rate have been optimistic. In this paper, we propose an attack on the LLO-CVQKD system that exploits the phase estimation error associated with the amplitude of the phase reference pulses. The corresponding change in the estimation of noise is used to leave freedom for Eve to obtain a considerably larger amount of information than that estimated by Alice and Bob. We call this attack the “reference pulse attack” (RPA).

*sr734@cam.ac.uk

This paper is organized as follows. In section II, we briefly describe the LLO-CVQKD system under the GMCS protocol and demonstrate the phase noise and secret key analysis. In section III, we present the reference pulse attack model and explain the excess noise tolerance that Eve makes use of to increase the scale of the attack. More importantly, we revisit the expression for the mutual information analysis under the reference pulse attack. In section IV, we display the simulation results on excess noise tolerance and mutual information as a function of attenuation coefficient and transmission distance. And we show the attack efficiency and possible countermeasures. Finally, conclusions are drawn in section V.

II The LLO CVQKD system

In this section, we describe the implementation of the LLO-CVQKD system and the current state-of-art noise model where we focus on the phase noise, especially the phase estimation error noise, to reveal the loophole.

A. Implementation principle

As shown in Fig. 1, a practical LLO-CVQKD system using the GMCS protocol can be analysed in four parts: Alice's preparation, channel propagation, Bob's detection and post processing.

First of all, Alice prepares a train of Gaussian modulated coherent states α_A with quadrature X_A and P_A with variance V_A . Then, she transmits these coherent states to Bob through the quantum channel, which induces an arbitrary phase rotation on the signal pulses. In order to recover the initial phase of the signal, a phase reference pulse, α_A^R , of quadrature X_A^R and P_A^R is transmitted along each signal pulse. The intensity of the reference pulse is a few orders greater than the signal variance. It is of great importance that the reference pulse amplitude is not too large to limit signal-reference pulse interference. The quantum channel is characterized by the channel parameters: transmittance T and excess noise ξ associated with the action from a malicious eavesdropper, Eve.

At Bob, quadrature of the signal and the reference pulses are measured with intense LO pulses using a shot-noise limited heterodyne detector with an efficiency η . Unlike the conventional CVQKD implementation, in the LLO-CVQKD system, a separate laser at Bob is applied to generate the LO. In order to robustly estimate the misalignment of the reference frames of the two free-running lasers, the mean reference pulses' quadrature values at Alice are publically announced. The quadrature measurement outcomes X_B^R and P_B^R of the reference pulse are associated with estimated rotation angle, $\widehat{\varphi}_R$, as given below:

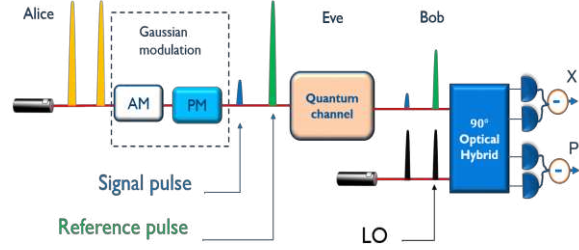


Fig.1 Practical LLO-CVQKD setup. The signal pulse (blue) and phase reference pulse (green) are transmitted through the optical channel and encounter same attenuation. At Bob, the received signals are interfered with the LO (black) to extract quadrature values.

$$X_B^R = \sqrt{\frac{T\eta}{2}} (X_A^R \cos \widehat{\varphi}_R + P_A^R \sin \widehat{\varphi}_R) \quad (1)$$

$$P_B^R = \sqrt{\frac{T\eta}{2}} (-X_A^R \sin \widehat{\varphi}_R + P_A^R \cos \widehat{\varphi}_R) \quad (2)$$

The estimation can be calculated straightforwardly without losing generality by preparing the initial reference pulse with a zero phase angle ($P_A^R = 0$).

$$\widehat{\varphi}_R = \tan^{-1} \left(\frac{P_B^R}{X_B^R} \right) \quad (3)$$

Consequently, the estimated phase angle is applied to rotate Alice's initial state quadrature or Bob's state quadrature values. This is followed by channel parameters estimation, error correction and privacy amplification.

B. Phase noise estimation

However, the phase rotation of the quantum signals cannot be completely corrected through the phase estimation of the reference pulse. As shown in Fig.2, the quantum signal phase rotation $\varphi_s = \theta_{SLO} - \theta_{SSource}$ is the phase difference between the quantum signal at Alice, $\theta_{SSource}$, and the local local oscillator, θ_{SLO} , at Bob. When reference pulses are deployed to estimate φ_s , the phase noise primarily originates from: (a) the phase drift due to the spectral linewidths, $\Delta\nu_A$, of the laser at Alice and $\Delta\nu_B$ of the laser at Bob; and (b) the deviation of estimated phase value, $\widehat{\varphi}_R$, of the reference pulse from the exact phase values φ_R .

Since the relative phase drift between two free running lasers can be modelled as a Gaussian stochastic process, centred at the central frequency, the variance of this phase drift at the time interval between quantum and reference pulses can be estimated from:

$$V_{drift} = \frac{2\pi(\Delta\nu_A + \Delta\nu_B)}{f_{rep}} \quad (4)$$

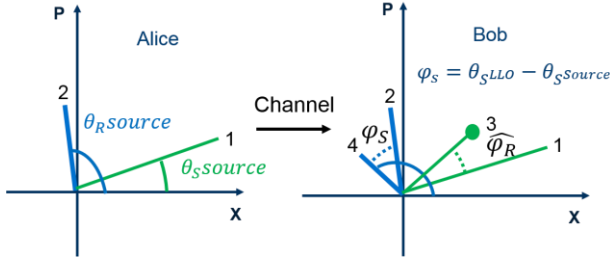


Fig.2 The general process of phase rotation and estimation. At Bob, the actual relative phase, ϕ_S , (blue angle) of the quantum signal (1,3) and estimated relative phase $\widehat{\phi}_R$ (green angle) from reference pulse (2,4) are added to initial phase. $\widehat{\phi}_R$ is used to estimate phase difference ϕ_S between two free-running lasers.

where f_{rep} is the repetition rate of the system.

Similarly, one can find the uncertainty, V_{error} , associated with the measured and the exact phase of the reference pulse, which is inversely proportional to the amplitude E_{Ref} of the reference pulse [24]. This is primarily due to the fundamental shot noise and total noise χ_t , and can be written as [21][24]:

$$V_{error} = var(\widehat{\phi}_R - \phi_R) = \frac{(\chi_t + 1)}{E_{Ref}^2} \quad (5)$$

Both these uncertainties, V_{drift} and V_{error} , contribute to the misalignment between Alice and Bob's reference frames and results in a total phase excess noise ξ_{phase} , which can be derived from ref. [20][21] as:

$$\begin{aligned} \xi_{phase} &\approx V_A * V_{phase} \quad (6) \\ &= V_A * \left(\frac{1 + \chi_t}{E_{Ref}^2} + 2\pi \frac{\Delta v_A + \Delta v_B}{f_{rep}} \right) \end{aligned}$$

Therefore, the phase excess noise is contributed from two parts: the former term is phase estimation error noise ξ_{error} and the last term is drift noise ξ_{drift} . The total excess noise ξ_t to favour easy understanding of our proposed attack, is therefore expressed as:

$$\xi_t = \xi_e + \xi_{phase} \quad (7)$$

where ξ_e comes from Eve's quantum signal interfering actions and other noises attributed to her account. Using the linear Gaussian model, the quadrature values measured by Bob is written as:

$$\begin{pmatrix} \widehat{X}_B \\ \widehat{P}_B \end{pmatrix} = \sqrt{\frac{T\eta}{2}} \left[\begin{pmatrix} \cos \widehat{\phi}_R & \sin \widehat{\phi}_R \\ -\sin \widehat{\phi}_R & \cos \widehat{\phi}_R \end{pmatrix} \begin{pmatrix} X_A \\ P_A \end{pmatrix} + \begin{pmatrix} \xi_{ex} + X_N \\ \xi_{ep} + P_N \end{pmatrix} \right] + \begin{pmatrix} x_{ele} \\ p_{ele} \end{pmatrix} \quad (8)$$

X_N and P_N are vacuum quadratures with unit shot noise variance (N_0). x_{ele} and p_{ele} are electronic noise quadratures with variance V_{ele} . In the above equation Eq. (8), the rotation matrix in the first term accounts the phase estimation error while the ξ_{ex} and ξ_{ep} represent the noise due to Eve's attack.

C. Secret key analysis

The secret key formula pertaining to the LLO-CVQKD scheme follows exactly that for a conventional CVQKD scheme. Under a collective attack [3] with reverse reconciliation, the key rate is:

$$K_{collective} = \beta I_{AB} - \chi_{BE} \quad (9)$$

Where β is the reconciliation efficiency and I_{AB} is the mutual information between Alice and Bob while χ_{BE} is the upper bound of Eve's information related to the Holevo bound [25]. From the Shannon equation, I_{AB} with heterodyne detection can be derived through:

$$I_{AB} = \log_2 \frac{V_B}{V_{B|A}} = \log_2 \frac{V + \chi_t}{1 + \chi_t} \quad (10)$$

Here, the total added noise χ_t referred to the input (at Alice) includes the channel χ_{line} and the heterodyne detection noise χ_{het} with included electronics noise.

$$\chi_{line} = \frac{1}{T} - 1 + \xi_t \quad (11)$$

$$\chi_{het} = \frac{[1 + (1 - \eta) + 2V_{ele}]}{\eta} \quad (12)$$

$$\chi_t = \chi_{line} + \frac{\chi_{het}}{T} \quad (13)$$

Furthermore, the accessed information by Eve χ_{BE} is evaluated using the Von Neumann entropy $S(\cdot)$ [26]:

$$\chi_{BE} = S(E) - S(E|B) \quad (14)$$

For the GMCS protocol, the entropy is analysed using the symplectic eigenvalues [27] of covariance matrix γ . Therefore, based on the formula given in [20][28], the general mutual information between Eve and Bob is:

$$\chi_{BE} = \sum_{i=1}^2 G\left(\frac{\lambda_i - 1}{2}\right) + \sum_{i=3}^5 G\left(\frac{\lambda_i - 1}{2}\right) \quad (15)$$

where $G(x) = (x + 1) \log_2(x + 1) - x \log_2 x$ and the eigenvalues $\lambda_{1,2} = \sqrt{\frac{1}{2}(A \pm \sqrt{A^2 - 4B})}$ with

$$A = V^2(1 - 2T) + 2T + T^2(V + \chi_{line})^2 \quad (16)$$

$$B = [T(V\chi_{\text{line}} + 1)]^2 \quad (17)$$

Considering that heterodyne detection, $\lambda_{3,4,5}$ can be expressed by $\lambda_{3,4} = \sqrt{\frac{1}{2}(C \pm \sqrt{C^2 - 4D})}$ and $\lambda_5 = 1$ with

$$C = \frac{1}{(T(V+\chi_t))^2} [A\chi_{\text{het}}^2 + B + 1 + 2\chi_{\text{het}}(V\sqrt{B} + T(V + \chi_{\text{line}})) + 2T(V^2 - 1)] \quad (18)$$

$$D = \left(\frac{V + \sqrt{B}\chi_{\text{het}}}{T(V + \chi_t)} \right)^2 \quad (19)$$

After analytically reviewing the current LLO-CVQKD system, the novel attack on this system is discovered and explained in following section.

III Reference pulse attack

A. Reference pulse attack model

In CVQKD, the parameter estimation procedure allows Alice to estimate only the overall excess noise value, ξ_t , as a single estimated value, of which contributions from several individual noise sources are practically impossible to distinguish. As a consequence, the variation in the noise contribution from individual noise sources cannot be detected if the overall excess noise is kept unchanged. We will exploit this vulnerability to facilitate the reference pulse attack.

The fundamental plan of the reference pulse attack is to manipulate individual excess noise contributions without altering the overall excess noise ξ_t . The attack works as follows. Eve attacks on the quantum signal pulses, which inevitably increases the overall excess noise. However, at the same time, she decreases the phase estimation error noise ξ_{error} , that is associated with the amplitude of the reference pulse, by an equivalent amount. Therefore, the total excess noise calculated by Eq. (7), remains unchanged. As a result, the overall excess noise estimated by Alice and Bob does not increase with additional attacks while extra information is successfully accessed by Eve without being realised.

Without loss of generality, we consider the reference pulse attack based on a typical fiber optic implementation of LLO-CVQKD system [20][21] as the schematic diagram shown in Fig.3. Let T and ξ_t be the estimated signal channel parameters which are used in Eq. (11) - Eq. (19) in order to estimate the I_{AB} -mutual information

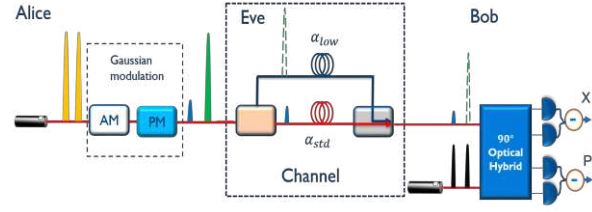


Fig.3 Reference pulse attack schematic diagram. At the output of Alice, Eve selectively switches the reference pulse to the low loss channel (blue) and the quantum pulse to the normal SMF fibre (red). She recombines the pulses at the input of Bob. The dashed green lines shows the less-attenuated path reference pulses.

between Alice and Bob, and the χ_{BE} -information acquired by Eve.

The reference pulse attack happens during the transmission of the pulses through the channel. After the quantum signals and the reference pulses are sent to the channel, at the output of Alice, Eve distinguishes and separates them into two individual channels. All quantum signals are transmitted through standard single mode fibre (SMF) with an attenuation factor $\alpha_{\text{std}} = 0.2\text{dB/km}$, while the reference pulses are transmitted through low loss channel of attenuation coefficient $\alpha_{\text{low}} < \alpha_{\text{std}}$. $\alpha_{\text{low}} = 0$ for zero loss (vacuum) channel while $\alpha_{\text{low}} = 0.14\text{dB/km}$ is currently achievable with hollow-core fibres [29]. At the input of Bob, Eve recombines the pulses into single SMF channel.

In addition to separating the signal and reference pulses and then recombining them, Eve also performs another simultaneous task. She increases her amount of attack on the signal pulses and gains more information. This will, however, increase the excess noise ξ_e by ξ_e^{RPA} which might be detected by the users as it results in an elevation in total excess noise ξ_t to ξ_t^{RPA} (Eq. (7)). As a consequence, this will lead to the estimation of new Holevo bound for Eve's information, $\chi_{BE}^{\text{actual}}$, by Alice and Bob. But, since the reference pulses propagate through low loss channel and reach Bob at an elevated amplitude, as we can see from Eq. (6), it will reduce the noise associated with phase estimation error noise. The noise increase in total excess noise is thus compensated, and Alice and Bob estimate after overall attack process χ_{BE}^{RPA} instead of $\chi_{BE}^{\text{actual}}$, hence underestimate Eve's information.

The additional amount of the information that Eve can steal without increasing total excess noise is, of course, limited by the channel loss of the reference pulses. We will quantify this in the following subsection.

B. Excess noise tolerance

For the success of the attack, the elevation in excess noise due to the attack on the signal must be compensated by simultaneous reduction in the phase excess noise. This requires the estimation of noise margin available to Eve from the reduction of phase estimation error noise that is associated with the amplitude of the reference pulse. From the Eq. (6), the reduced phase estimation error noise ξ_{error}^{low} can be evaluated as:

$$\xi_{error}^{low} = V_A * \frac{\chi_t + 1}{\eta * T_{low} E_{Ref}^2} = \xi_{error}^{std} * \frac{T_{std}}{T_{low}} \quad (20)$$

where, T_{std} is the transmittance of SMF fibre with attenuation coefficient $\alpha_{std} = 0.2\text{dB/km}$ and T_{low} is transmittance of the low loss reference pulse channel with attenuation coefficient $\alpha_{low} < \alpha_n$. The available phase excess noise tolerance that Eve can account for by the attack can be evaluated as:

$$\begin{aligned} \xi_{tole} &= \xi_{error}^{std} - \xi_{error}^{low} \\ &= V_A * \frac{\chi_t + 1}{E_{Ref}^2} * \left(1 - \frac{1}{10^{\frac{(\alpha_{std} - \alpha_{low}) * L}{10}}}\right) \end{aligned} \quad (21)$$

Here, we assume the length L of the quantum channel and reference channel are equal. Based on the value α_{low} of the reference channel and channel length L, Eve can increase her attack until the additional excess noise ξ_e^{RPA} equals ξ_{tole} . Hence the resultant phase noise is unchanged. Under the scope of reference pulse attack, we can rewrite Eq. (7) as:

$$\xi_t^{post} = \xi_e + \xi_e^{RPA} + \xi_{phase} - \xi_{tole} \quad (22)$$

As explained earlier, the first two noise terms ($\xi_e + \xi_e^{RPA}$) are attributed to Eve's attack on the signal while the last two terms ($\xi_{phase} - \xi_{tole}$) represent the phase noise linked to the reference pulse. Under the reference pulse attack, the quadrature values measured by Bob, Eq. (10) can be rewritten as:

$$\begin{aligned} \begin{pmatrix} \overline{X_B^{RPA}} \\ \overline{P_B^{RPA}} \end{pmatrix} &= \sqrt{\frac{T\eta}{2}} \left[\begin{pmatrix} \cos \widehat{\varphi_{RPA}} & \sin \widehat{\varphi_{RPA}} \\ -\sin \widehat{\varphi_{RPA}} & \cos \widehat{\varphi_{RPA}} \end{pmatrix} \begin{pmatrix} X_A \\ P_A \end{pmatrix} \right. \\ &\quad \left. + \begin{pmatrix} \xi_{ex} + \xi_{add} + X_N \\ \xi_{ep} + \xi_{add} + P_N \end{pmatrix} \right] + \begin{pmatrix} x_{ele} \\ p_{ele} \end{pmatrix} \end{aligned} \quad (23)$$

Under the reference pulse attack, the phase estimator φ_{RPA} is more accurate and lowers the phase estimation error noise while additional excess noise induced on the

signal by Eve keeps the measured quadrature values unchanged. In the following section, we estimate Eve's gain in information during the attack.

C. Secret key analysis under attack

In this section, a comparison of the mutual information and Holevo bound for Eve's gain before (I_{AB} and χ_{BE}) and after the attack (I_{AB}^{RPA} and χ_{BE}^{RPA}) are considered. Based on eq. (22), the total noise estimated by Alice and Bob after attack, χ_t^{RPA} , is identical to the 'no' attack situation χ_t . This indicates that the attack, as in Eq. (10), does not affect the mutual information between Alice and Bob which can be referred to as:

$$I_{AB} = \log_2 \frac{V + \chi_t}{1 + \chi_t} = \log_2 \frac{V + \chi_t^{RPA}}{1 + \chi_t^{RPA}} = I_{AB}^{RPA} \quad (24)$$

Similarly, the Holevo bound for Eve's information estimated by Alice and Bob is unchanged, as long as the total noise remains the same, ie $\chi_{BE} = \chi_{BE}^{RPA}$. However, the actual information obtained by Eve χ_{BE}^{actual} is greater than χ_{BE} due to her additional signal extraction actions whose excess noise is compensated by the phase noise reduction. An easy and straight forward way to estimate χ_{BE}^{actual} is to consider the total noise without phase noise reduction in Eq. (22), i.e., $\xi_t^{actual} = \xi_e + \xi_e^{RPA} + \xi_{phase}$. By following the exact procedure, from Eq. (11) to Eq. (19) we can estimate and find that $\chi_{BE}^{actual} > \chi_{BE}$. We define the efficiency of the reference pulse attack as the ratio of the information leaked to Eve with and without attack:

$$K_{eff} = \frac{\chi_{BE}^{actual} - \chi_{BE}}{I_{AB} - \chi_{BE}} \quad (25)$$

The following section reports the results of the phase noise reduction and attack efficiency under different LLO-QKD system conditions.

IV attack performance analysis

We investigate the attack performance as a function of various reference channel attenuation factors, α_{low} , ranging from the vacuum channel (0dB/km) to conventional SMF (0.2dB/km). We also consider a practical scenario where the reference channel uses recently reported hollow-core fibres of 0.1419dB/km attenuation coefficient. The simulation parameters are selected to match the parameters used in recent LLO-CVQKD experiments [20][22], which are: variance of Alice's modulation $V_A = 4$, the efficiency of the reconciliation process $\beta = 0.97$, the detector efficiency $\eta = 0.5$, the signal path fibre attenuation coefficient $\alpha_{std} = 0.2\text{dB/km}$, the electronic noise

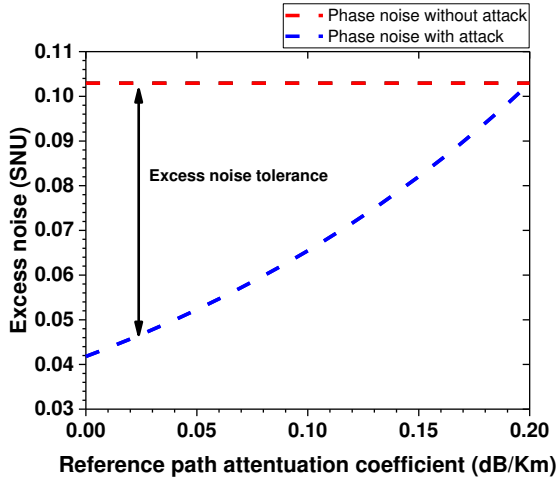


Fig. 4 Phase noise with (blue dashed line) and without (red dashed line) attack variation at different reference path attenuation coefficient. Considerable excess noise tolerance is generated by attack. Simulations are performed in the collective attack and $V_A=4$, $A_R^2/V_A = 100$ and $L = 20\text{Km}$.

$V_{elec} = 0.01$, the original system excess noise $\xi_e = 0.01$, the receiver repetition rate $f_{rep} = 100\text{MHz}$, laser linewidth $\Delta\nu = 1.9\text{kHz}$ and the realistic reference pulse amplitude E_R which is chosen as $E_R^2/V_A = 100$. Values are expressed in shot noise unit.

Fig. 4 shows the variation in phase excess noise tolerance (Eq. (21)) with different attenuation coefficients of the reference channel for a 20km LLO-CVQKD link. It can be seen that, the phase noise reduces by 58% and 23% of the initial value for zero loss and hollow core fibre reference channel respectively.

The actual and estimated mutual information between Alice and Bob and the Holevo bound for Eve's information are shown in Fig.5 for different values of reference path attenuation coefficients, α_{low} , for a 20km channel length. I_{AB} (black dashed line) is independent of the attack. A region (light red area) appears between actual Eve accessed information χ_{BE}^{actual} (blue dashed line) and the estimated value χ_{BE}^{RPA} (red dashed line) after overall process, which is referred to as the attack-induced insecure region. The χ_{BE}^{RPA} is independent of α_{low} . The truly secure region (blue area) is secure under the attack.

In this case, for a 20 km distance and for 0dB/km attenuation coefficient, Eve can extract 79% of the secret key without being found. For a feasible 0.14dB/km attenuation coefficient, Eve can achieve 37% information extraction from original secure key region.

Fig. 6 shows the mutual information variation as a function of transmission distance L . Rather than for a range of attenuation factors, the χ_{BE}^{actual} values are only evaluated for $\alpha_{low} = 0\text{ dB/km}$ (blue dashed line) and

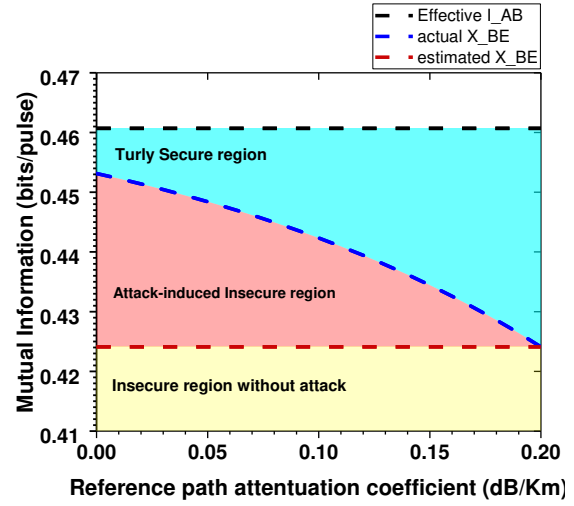


Fig.5 Mutual information variations for different reference path attenuation coefficients. Simulations are performed for collective attack, with $V_A=4$, $A_R^2/V_A = 100$ and $L = 20\text{Km}$. The excess information obtained by Eve is shown in red region.

0.14 dB/km (red dashed line). The estimated Eve's information from Alice and Bob after the overall attack, χ_{BE}^{RPA} , is evaluated at a reference path attenuation coefficient $\alpha_{std} = 0.2\text{ dB/km}$ (purple solid line). The mutual information between Alice and Bob, I_{AB} (black solid line), monotonically decreases as a function of

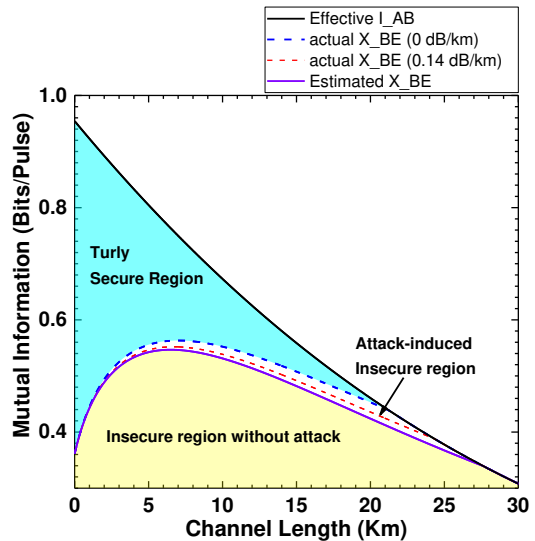


Fig. 6 Mutual information vs channel lengths. Insecure region expands with increase in transmission distance. Zero-loss (vacuum) channel maximize the information gain by Eve. Simulations are performed in the collective attack and the $V_A=4$, $A_R^2/V_A = 100$

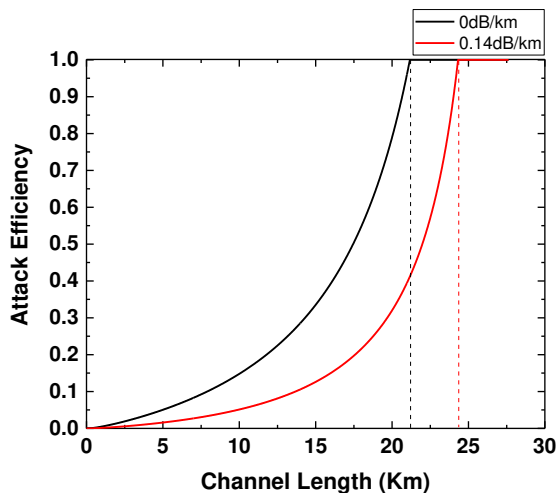


Fig. 7 Attack efficiency vs channel lengths. The insecure key ratio rises with transmission distance increasing. The results from zero-loss (vacuum) channel and the realistic lowest hollow-core fibre channel are collected. 100% attack efficiency is achieved from 21.2km and 24.3 km for 0 and 0.14 dB/km attenuation factors.

channel length. The secure region under attack is labelled as the truly secure region while the yellow region is the insecure region estimated by Alice and Bob with or without attack. The white region referred as the attack induced insecure region indicating that secret keys are being successfully obtained by Eve without being detected. The attack-induced insecure key region broadens as the signal transmission distance increases. This result shows the mounting disparity between the quantum channel and the reference channel loss.

At a relatively long distance, the unsecured key ratio grows rapidly which indicates an increase in attack efficiency. We need to emphasize that the exact K_{eff} value varies with system parameters and a 100% insecure key situation can be achieved especially at long transmission distance. For example, from Fig.7, it can be seen, for $\alpha_{low} = 0\text{dB/km}$, the attack efficiency, K_{eff} becomes 100% at a quantum channel distance around 21.2 km. While considering the realistic value of $\alpha_{low} = 0.14\text{dB/km}$, K_{eff} reaches 100% at 24.3 km, above which no security can be promised. The null key distance for a standard SMF channel is 27.6km for the given set of system parameters.

We propose plausible countermeasures in order to detect the reference pulse attack. Bob can monitor the instantaneous amplitude of the reference pulse and compare it with the value at the output of Alice. If the ratio has a large disparity with $\sqrt{T_{std}}$ - obtained from parameter estimation of the signal, Alice and Bob can simply stop communication. Otherwise, we may could recalculate the

upper bound of χ_{BE} by including tolerable phase noise, ξ_{tole} , Eq. (21). This would guarantee the fully trusted key under reference pulse attack. A rigorous countermeasure analysis will follow this paper.

V Conclusion

In this paper, we have, for the first time, revealed a security threat in a LLO-CVQKD system arising from the quantum uncertainty of reference pulses which is employed as pilot signals to estimate phase noise between two free-running lasers. We have proposed a novel attack on the LLO-CVQKD system, named as the reference pulse attack. This comprises of two simultaneous tasks: (a) where Eve selectively switches reference pulse to low loss channel; and (b) attacks the quantum signals. We have shown that the phase estimation error noise can be tuned by adjusting the reference channel attenuation coefficient which provides Eve with an excess noise tolerance to acquire extra information from the quantum signals. More importantly, this estimation error exists in all reference pulse protocols so that the loophole could affect all of the LLO-CVQKD system configurations. Our proposed attack breaks the immunity of LLO-CVQKD that originally has been proposed to defend the attack on local oscillator. It should be noted that with a relatively larger reference pulse amplitude the efficiency of the attack would be much lower than that obtained in this paper. However, in general, the current implementation of LLO-CVQKD systems are vulnerable to the reference pulse attack.

VI. Acknowledgment

This work has been supported by the Quantum Communication Hub through EPSRC UK National Quantum Technology Programme (UKNQTP) fund EP/M013472/1.

-
- [1]. C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (IEEE, New York, 1984), pp. 175–179.
 - [2]. A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. 67, 661 (1991).

- [3]. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The Security of Practical Quantum Key Distribution, *Rev. Mod. Phys.* 81, 1301 (2009).
- [4]. H.-K. Lo, M. Curty, and K. Tamaki, Secure Quantum Key Distribution, *Nat. Photonics* 8, 595 (2014).
- [5]. Grosshans, Frédéric, et al. "Quantum key distribution using gaussian-modulated coherent states." *Nature* 421.6920 (2003): 238-241.
- [6]. Leverrier, Anthony, and Philippe Grangier. "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation." *Physical review letters* 102.18 (2009): 180504
- [7]. Weedbrook, Christian, et al. "Gaussian quantum information." *Reviews of Modern Physics* 84.2 (2012): 621.
- [8]. Diamanti, Eleni, and Anthony Leverrier. "Distributing secret keys with quantum continuous variables: principle, security and implementations." *Entropy* 17.9 (2015): 6072-6092.
- [9]. Huang, Duan, et al. "High-speed continuous-variable quantum key distribution without sending a local oscillator." *Optics letters* 40.16 (2015): 3695-3698.
- [10]. Chi, Yue-Meng, et al. "A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution." *New Journal of Physics* 13.1 (2011): 013003.
- [11]. Huang, Duan, et al. "A wideband balanced homodyne detector for high speed continuous variable quantum key distribution systems." *Third International Conference on Quantum Cryptography*, Waterloo, Canada. 2013.
- [12]. Orioux, Adeline, and Eleni Diamanti. "Recent advances on integrated quantum communications." *Journal of Optics* 18.8 (2016): 083002.
- [13]. Kumar, Rupesh, Hao Qin, and Romain Alléaume. "Coexistence of continuous variable QKD with intense DWDM classical channels." *New Journal of Physics* 17.4 (2015): 043027
- [14]. Garcia-Patron, Raul, and Nicolas J. Cerf. "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution." *Physical review letters* 97.19 (2006): 190503.
- [15]. Navascués, Miguel, Frédéric Grosshans, and Antonio Acín. "Optimality of Gaussian attacks in continuous-variable quantum cryptography." *Physical review letters* 97.19 (2006): 190502.
- [16]. Leverrier, Anthony, Frédéric Grosshans, and Philippe Grangier. "Finite-size analysis of a continuous-variable quantum key distribution." *Physical Review A* 81.6 (2010): 062343.
- [17]. Ma, Xiang-Chun, et al. "Enhancement of the security of a practical continuous-variable quantum-key-distribution system by manipulating the intensity of the local oscillator." *Physical Review A* 89.3 (2014): 032310.
- [18]. Huang, Jing-Zheng, et al. "Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack." *Physical Review A* 87.6 (2013): 062329.
- [19]. Qin, Hao, Rupesh Kumar, and Romain Alléaume. "Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution." *Physical Review A* 94.1 (2016): 012325.
- [20]. Qi, Bing, et al. "Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection." *Physical Review X* 5.4 (2015): 041009.
- [21]. Soh, Daniel BS, et al. "Self-referenced continuous-variable quantum key distribution protocol." *Physical Review X* 5.4 (2015): 041010
- [22]. Huang, Duan, et al. "High-speed continuous-variable quantum key distribution without sending a local oscillator." *Optics letters* 40.16 (2015): 3695-3698.
- [23]. Kleis, S., Rueckmann, M., & Schaeffer, C. G. (2017). Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals. *Optics Letters*, 42(8), 1588-1591.
- [24]. Marie, A., & Alléaume, R. (2017). Self-coherent phase reference sharing for continuous-variable quantum key distribution. *Physical Review A*, 95(1), 012316.
- [25]. Holevo, Alexander Semenovich. "Bounds for the quantity of information transmitted by a quantum communication channel." *Problemy Peredachi Informatsii* 9.3 (1973): 3-11.
- [26]. Von Neumann, John. *Mathematical foundations of quantum mechanics*. No. 2. Princeton university press, 1955.
- [27]. Adesso, Gerardo, Alessio Serafini, and Fabrizio Illuminati. "Extremal entanglement and mixedness in continuous variable systems." *Physical Review A* 70.2 (2004): 022318.
- [28]. Fossier, Simon, et al. "Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers." *Journal of Physics B: Atomic, Molecular and Optical Physics* 42.11 (2009): 114014.
- [29]. Tamura, Yoshiaki, et al. "Lowest-ever 0.1419-dB/km loss optical fiber." *Optical Fiber Communication Conference*. Optical Society of America, 2017.