SCIENTIFIC REPORTS
nature research

OPEN

Practical Security Analysis of Reference Pulses for Continuous-Variable Quantum Key Distribution

Wei Zhao, Ronghua Shi & Duan Huang*

By manipulating the reference pulses amplitude, a security vulnerability is caused by self-reference continuous-variable quantum key distribution. In this paper, we formalize an attack strategy for reference pulses, showing that the proposed attack can compromise the practical security of CVQKD protocol. In this scheme, before the beam splitter attack, Eve intercepts the reference pulses emitted by Alice, using Bayesian algorithm to estimate phase shifts. Subsequently, other reference pulses are re-prepared and resubmitted to Bob. In simulations, Bayesian algorithm effectively estimates the phase drifts and has the high robustness to noise. Therefore, the eavesdropper can bias the excess noise due to the intercept-resend attack and the beam splitter attack. And Alice and Bob believe that their excess noise is below the null key threshold and can still share a secret key. Consequently, the proposed attack shows that its practical security can be compromised by transmitting the reference pulses in the continuous-variable quantum key distribution protocol.

Quantum key distribution (QKD) is one of the advanced technology to date, and the security of the shared keys is guaranteed by the quantum mechanics[1–5]. Allowing two authenticated parties to establish secret keys in an insecure channel, QKD provides a secure way. In the discrete-variable quantum key distribution (DVQKD), several significant achievements have been achieved[6–12]. For implementing DVQKD, Pan *et al*. has launched a low-Earth-orbit satellite, with key rate around 20 orders of magnitudes greater than optical fiber[13]. For decades, continuous-variable quantum key distribution (CVQKD) without the requirement of single-photon detection, has made significant progress of QKD research[14–16]. However, there is a fundamental limit on the maximum number of secret bits that can be generated by two remote parties. This limit is the secret key capacity of the lossy channel, which also known as the PLOB bound[17]. In this general context, Gaussian-modulated coherent state (GMCS) protocol has been experimentally achieved both in long distance and high speed[18–21]. Moreover, the protocol has already proved secure in the asymptotic regime[22,23] and finite-size regime[24,25]. To be specific, the signal pulses and local oscillator (LO) pulses are simultaneously prepared by Alice in the GMCS protocol. In other words, the LO is deemed as a fixed phase reference for the signal detection, which can reduce the phase noise.

Nevertheless, the transmission of the LO brings about several limitations[26–29]. Firstly, the LO may be controlled and modified by eavesdropper. Eve may launch attacks by manipulating the LO, such as LO fluctuation attacks[30], calibration attacks[31], saturation attacks[32] and wavelength attacks[28,33]. Secondly, the complicated techniques of multiplexing and de-multiplexing are necessary to transmit and separate the two pulses, respectively. Thirdly, sending the strong LO pulses can reduce the transmission efficiency. In order to solve these problems, self-reference CVQKD protocols are proposed, which can generate the LO locally at Bob's side. Besides, several protocols have been proposed to solve the flaws of phase drift in the self-reference CVQKD protocol[34–36].

Recently, Qin *et al*. formalize an attack strategy; Eve cuts down the quantum channel and inserts an external light into the self-reference CVQKD system[37]. However, the countermeasure for this attack is proposed in the reference[38]. Shengjun *et al*. propose a reference pulse attack, which can exploit the phase estimation error associated with the reference pulses to attack the self-reference CVQKD protocol[39]. Besides, Pereira *et al*. consider an attack on a coherent-state protocol; Eve not only taps the main communication channel but also hacks AliceâĂŹs device[40]. Nevertheless, there are some defects in theoretical analysis and it is hard to achieve. Inspired by side channel attack, we formalize the attack strategy for discrete-modulated and Gaussian-modulated self-reference CVQKD, respectively. The attack works as follows: Eve increases her amount of beam splitter attack on the quantum signal, which inevitably increasing the excess noise. Before the beam splitter attack, she utilizes the

School of Computer Science and Engineering, Central South University, Changsha, 410083, China. *email: duan.huang@foxmail.com

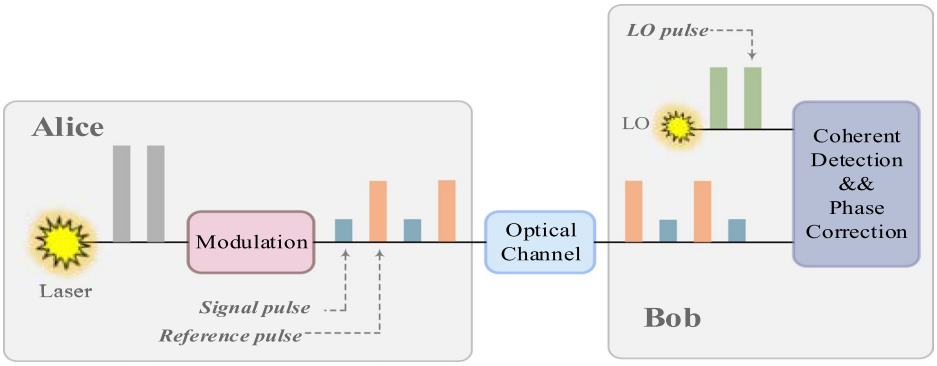


Figure 1. The self-reference CVQKD protocol. Alice sequentially sends reference pulses and signal pulses. At the receiver, Bob uses its own LO pulses to perform coherent detection. Here, LO represents the local oscillator.

intercept-resend attack and the Bayesian algorithm to decrease the phase estimation error noise. Therefore, Eve can bias the excess noise due to the beam splitter attack and the intercept-resend attack, and Alice and Bob believe their excess noise estimation is below the null key threshold and they can still share a secret key. To intercept-resend attack, that is, Eve can monitor and intercept the reference pulses emitted by Alice. Subsequently, she measures each reference pulse and then estimates the phase drift using the Bayesian algorithm. After phase estimation and compensation operation, she re-prepares and resubmits another reference pulses, which is sent to Bob. What's more, we propose to utilize Bayesian algorithm to estimate the reference pulses. The algorithm not only can obtain a confidence interval, but also has robustness to noise. Therefore, the algorithm can increase the accuracy of phase estimation for Eve. This series of operations can cause a security vulnerabilities through the manipulation of the reference pulses.

Practical Security Analysis

In this section, we start by describing the protocol of the self-reference CVQKD. Subsequently, we analyze how Eve can intercept the reference pulses and estimate the phase drift for the discrete-modulated and Gaussian-modulated self-reference CVQKD, respectively. The self-reference CVQKD protocol, as shown in Fig. 1, consists of two parts, one is the coherent states preparation and propagation, and the other part is the coherent states detection and processing. At the transmitter, Alice prepares the Gaussian-modulated coherent states (or the discrete-modulated states) and then transmits to Bob. The arbitrary phase drift of the states will be inevitably induced through the quantum channel. Therefore, the phase reference pulses are necessary to transmit along with the signal pulses. As depicted in Fig. 1, the reference pulses and signal pulses are sent by Alice alternatively and periodically. At the receiver, Bob can utilize the relatively strong reference pulses to estimate the phase[35]. In theory, quantum phase noise $\Delta\phi$ between the two users can be written as[41]

$$\Delta\phi \approx \frac{2\pi}{s}\Delta\nu L, \tag{1}$$

where L represents the length of the fiber, $\Delta\nu$ is the difference frequency between the user's lasers, and s denotes the speed of light in the fiber. Although several protocols are proposed to the phase compensation, the strong reference pulses are still indispensable in the self-reference CVQKD. However, propagating the relatively strong reference pulses may result in security vulnerabilities.

In what follows, we analyze the practical security of reference pulses for CVQKD with discrete modulation. In this scenario, Eve has the ability to monitor and intercept the reference pulses from Alice to Bob. Basically, Eve measures each reference pulse and estimates the phase drift emitted by Alice. After the phase compensation, she re-prepares and resubmits reference pulses, which are sent to Bob. Next, we introduce how Eve employs Bayesian algorithm to estimate the phase drift of the intercepted reference pulses. Without loss of generality, we analyze the four-state self-reference CVQKD protocol[42–44]. The four-state can be denoted as $|\alpha_k\rangle = |\alpha e^{i(2k+1)\pi/4}\rangle$ with $k \in \{0, 1, 2, 3\}$, and the modulation variance is $V = 1 + 2\alpha^2$. When Eve intercepts reference pulses through the noisy channel, as shown in Fig. 2, the photon number resolving detector (PNRD) performs the measurement operation. Specifically, the measurement outcomes are denoted as $\mathscr{E} \in \{|\alpha_0\rangle, |\alpha_1\rangle, |\alpha_2\rangle, |\alpha_3\rangle\}$, and the total number of detected photons are described as $\mathscr{N} = \sum_{i=0}^{3} n_i$, where n_i symbolizes the detected photon of state $|\alpha_i\rangle$. Then, we provide the critical process of Bayesian estimation. Above all, in order to estimate the correct eigenphase, an initial prior probability distribution $\mathscr{P}(\phi)$ is provided to express the confidence interval that the current hypotheses is the correct eigenphase. Subsequently, the mean μ and its standard derivation σ are updated on the basis of the measurement results of PNRD. What's more, the posterior probability distribution can be calculated as[45,46]

$$\mathscr{P}(\phi|\mathscr{E}) = \frac{\mathscr{P}(\mathscr{E}|\phi)\mathscr{P}(\phi)}{\int \mathscr{P}(\mathscr{E}|\phi)\mathscr{P}(\phi)\mathrm{d}\phi}. \tag{2}$$

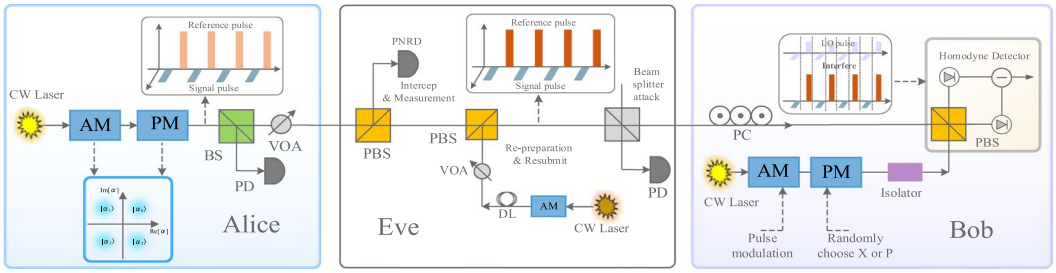


Figure 2. The practical security analysis of reference pulses for the CVQKD protocol with discrete modulation. CW laser, continuous wave laser; BS, beam splitter; PD, photodetector; VOA, variable optical attenuator; PBS, polarizing beam splitter; Att., attenuator; PNRD, photon number resolving detector; DL, delay line; PC, polarization controller; AM-PM, amplitude and phase modulation.

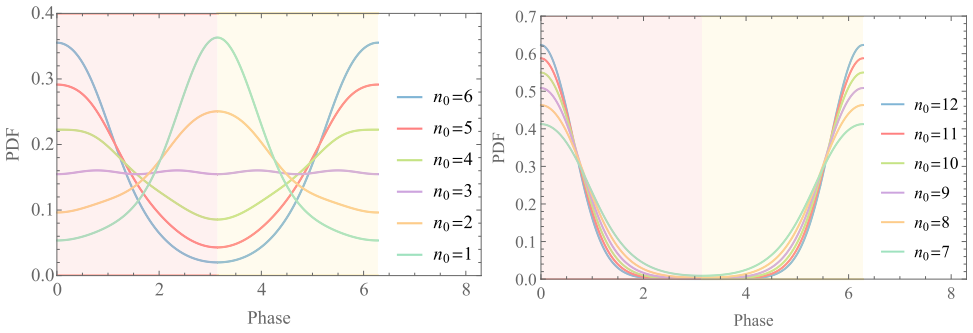


Figure 3. Probability density function (PDF) versus the phase drift.

Specifically, some particles drawn from the $\mathscr{P}(\phi)$ mismatch the likelihood function, which will be discarded later. The likelihood function is defined as $\mathscr{P}(|\alpha_0\rangle|\phi) = \frac{1}{4}(1 + e^{-\Delta^2}\cos(\phi))$, $\mathscr{P}(|\alpha_1\rangle|\phi) = \frac{1}{4}(1 + e^{-\Delta^2}\sin(\phi))$, $\mathscr{P}(|\alpha_2\rangle|\phi) = \frac{1}{4}(1 - e^{-\Delta^2}\cos(\phi))$ and $\mathscr{P}(|\alpha_3\rangle|\phi) = \frac{1}{4}(1 - e^{-\Delta^2}\sin(\phi))$. Without loss of generality, the qubit undergoes a phase diffusion process whose amplitude is characterized by the parameter Δ. After obtaining the posterior distribution in Eq. 2, we set the posterior probability distribution to equal the prior probability distribution. This updating program can be deemed as the iterative processing for each of the emulation.

Subsequently, we provide the mathematical definition of probability density function (PDF) to illustrate the relation between the phase shift and the detected photons $\mathscr{N}$. The PDF is defined as $\mathscr{P}_B(\phi; \mathscr{N}) = \frac{\sum_{i=0}^{3}\mathscr{P}(|\alpha_i\rangle|\phi)^{n_i}}{\mathscr{M}}$, where $\mathscr{M}$ is the normalization factor satisfies with $\int_0^{2\pi}\mathscr{P}_B(\phi; \mathscr{N})\mathrm{d}\phi = 1$. The simulation results of phase drift are depicted in Fig. 3. The two subgraphs illustrate that, the phase drift tends to zero if we increase the number of n_0 (where n_1, n_2 and n_3 are constant). Here, n_i is defined in the previous paragraph. Consequently, increasing the detected photons for intercepted reference pulses can improve the accuracy of phase estimation, thus reducing the possibility of phase shift. Next, we describe the main implementation steps of the Bayesian algorithm. In the initial interation of the algorithm, a prior distribution $\mathscr{N}(\mu_0, \sigma_0)$ is to express the confidence interval. Then, the dataset is utilized to update the μ and σ of the posterior probability distribution in accordance with Bayes' theorem. The parameter estimation for the inferred σ^2 of the posterior probability density is simulated in Fig. 4a, and the shaded region stands for the proportion correct ratio of the predicted trials. In other words, increasing the signal intensity level can improve the proportion correct of concentration. As shown in Fig. 4b, we utilize the different initial σ^2 to simulate and test that the performance is insensitive to the initial σ^2. In other words, the Bayesian algorithm has the high robustness. Furthermore, the main steps of the algorithm[45,47,48] are described in the Appendix.

By comparison to the discrete-modulated CVQKD protocol, the Gaussian-modulated CVQKD protocol is more complicated. We adopt the Mach-Zehnder (MZ) interferometer to estimate the phase drifts[49–53]. The Mach-Zehnder interferometer, as shown in Fig. 5, has two inputs labelled 1 and 2, one input is the intercepted reference pulses, and the other is the coherent light source. The two inputs are combined in two beamsplitters (BS_1 and BS_2) and two internal arms. On the one of the branches for output, a beamsplitter (BS_3) has two outputs labelled as 3 and 4. On the other branch, a beamsplitter (BS_3) has two outputs labelled as 5 and 6. According to the mentioned above, photodetectors are applied to outputs and respond to intensities I_k. Therefore, we integrate over some observations T, and define the parameter $W_k = \int_T I_k\,\mathrm{d}t$ with $k \in \{3, 4, 5, 6\}$. Particularly, the parameter W_k can be substituted by the integer n_k, where n_k represents the photodetection result in the time interval T. Based on the NFM theory (Noh, Fougères and Mandel)[51], the unambiguous value of phase ϕ is estimated as

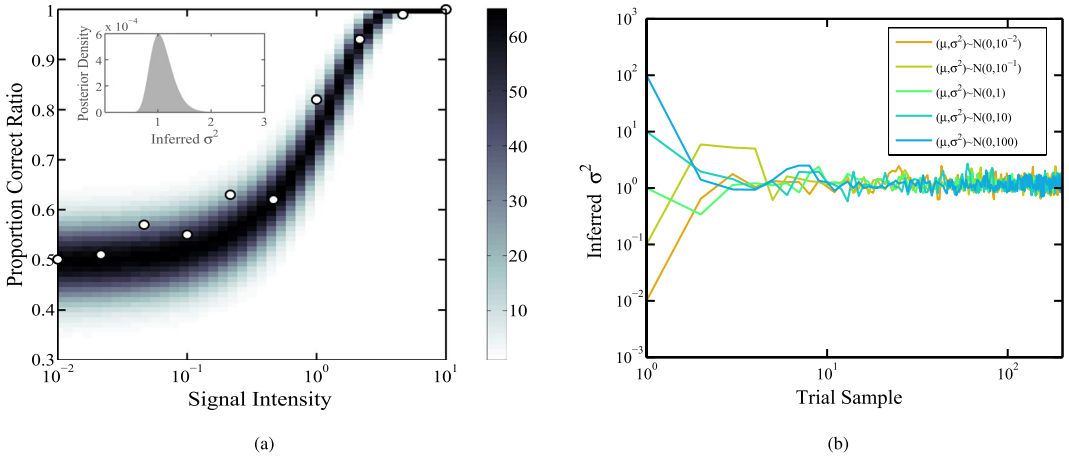


Figure 4. (**a**) The prediction model. A set of data points are performed in the simulation to estimate the phase variance by Bayesian phase estimation algorithm. (**b**) The parameter procedure with the different σ^2.

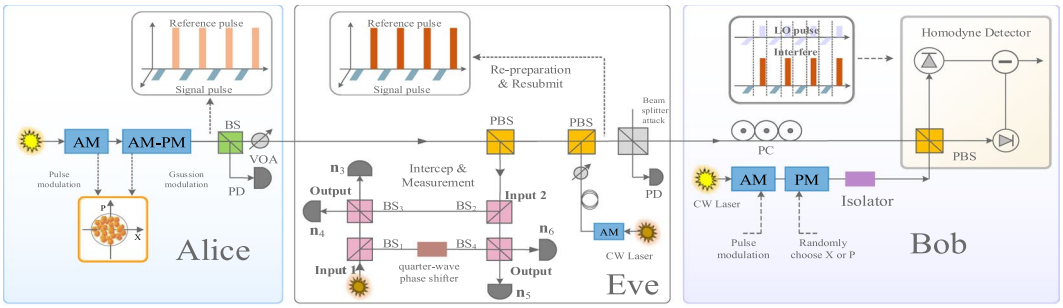


Figure 5. The practical security analysis of reference pulses for the CVQKD protocol with Gaussian modulation. CW laser, continuous wave laser; BS, beam splitter; PD, photodetector; VOA, variable optical attenuator; PBS, polarizing beam splitter; Att., attenuator; PNRD, photon number resolving detector; DL, delay line; PC, polarization controller; AM, amplitude modulation; PM, phase modulation.

$$\cos\phi = \frac{n_3 - n_4}{[(n_3 - n_4)^2 + (n_5 - n_6)^2]^{1/2}}, \quad \sin\phi = \frac{n_5 - n_6}{[(n_3 - n_4)^2 + (n_5 - n_6)^2]^{1/2}}. \tag{3}$$

When the photon number $\bar{n}_{\text{in}}$ at input 1 and 2 is determined, the outputs 3~6 have the mean values $\bar{n}_3 = \bar{n}_{\text{in}}(1 + V\cos\phi)$, $\bar{n}_4 = \bar{n}_{\text{in}}(1 - V\cos\phi)$, $\bar{n}_5 = \bar{n}_{\text{in}}(1 + V\sin\phi)$ and $\bar{n}_6 = \bar{n}_{\text{in}}(1 - V\sin\phi)$, where the maximum likelihood estimate can be given by

$$\hat{V} = \sqrt{\left(\frac{n_3 - n_4}{n_3 + n_4}\right) + \left(\frac{n_5 - n_6}{n_5 + n_6}\right)^2}. \tag{4}$$

Consequently, based on the Poissonian distribution of photoncount and mean value $\bar{n}_{\text{in}}$, the likelihood of ϕ and $\bar{n}_{\text{in}}$ is

$$\mathscr{P}(\mathbf{n}|\phi, \bar{n}_{\text{in}}) \propto (\bar{n}_{\text{in}})^{\sum n_k} e^{-2\bar{n}_{\text{in}}}(1 + V\cos\phi)^{n_3}(1 - V\cos\phi)^{n_4}(1 + V\sin\phi)^{n_5}(1 - V\sin\phi)^{n_6}, \tag{5}$$

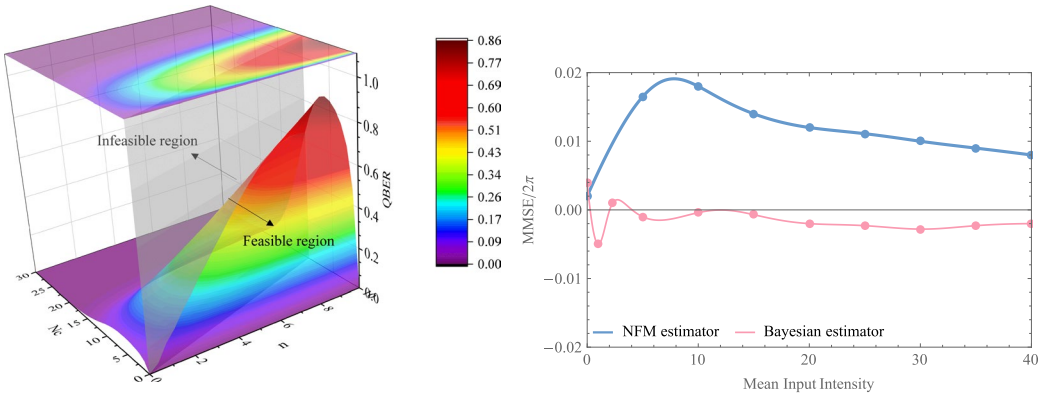
with the notation $\mathbf{n} = [n_3, n_4, n_5, n_6]$. Assuming that $\bar{n}_{\text{in}}$ is independent of ϕ and V, we have

$$\mathscr{P}(\mathbf{n}|\phi) = \int \mathscr{P}(\mathbf{n}|\phi, \bar{n}_{\text{in}})\mathscr{P}(\bar{n}_{\text{in}})\mathrm{d}\bar{n}_{\text{in}} \propto (1 + V\cos\phi)^{n_3}(1 - V\cos\phi)^{n_4}(1 + V\sin\phi)^{n_5}(1 - V\sin\phi)^{n_6}. \tag{6}$$

Consequently, the posterior probability distribution takes the following form

$$\mathscr{P}(\phi|\mathbf{n}) = \frac{\mathscr{P}(\mathbf{n}|\phi)\mathscr{P}(\phi)}{\int \mathscr{P}(\mathbf{n}|\phi)\mathscr{P}(\phi)\mathrm{d}\phi}, \tag{7}$$

which is in accordance with the Eq. 2 of four-state self-reference CVQKD protocol.



(a) (b)

Figure 6. (**a**) The QBER of the intercept-resend attack with the discrete modulation protocol. (**b**) Difference in minimum mean squared error for the two phase estimation schemes, namely the NFM estimator protocol[51,53,54], and Bayesian estimator protocol, respectively. Here, the phase shift is set as $\pi/3$.

Performance Analysis

First of all, we define transmission probability and transition probability to analyze the performance of the reference pulses for the discrete modulation protocol. In the four-state self-reference CVQKD protocol, there are four kinds of the intercepted encoding phase, namely the $\phi_i = \frac{(2k+1)\pi}{4}$, with $k \in \{0, 1, 2, 3\}$. According to the likelihood function, if the transmission states are in consistent with the measurement outcome $\mathscr{E}$, the equation can be simplified as

$$\begin{aligned}
\mathscr{P}(|\alpha_0\rangle|\phi_0) &= \frac{1}{4}(1 + e^{-\Delta^2}\cos(\pi/4)) \\
&= \frac{1}{4}\left(1 + \frac{\sqrt{2}}{2}e^{-\Delta^2}\right), \\
\mathscr{P}(|\alpha_1\rangle|\phi_1) &= \frac{1}{4}(1 + e^{-\Delta^2}\sin(3\pi/4)) \\
&= \frac{1}{4}\left(1 + \frac{\sqrt{2}}{2}e^{-\Delta^2}\right), \\
\mathscr{P}(|\alpha_2\rangle|\phi_2) &= \frac{1}{4}(1 - e^{-\Delta^2}\cos(5\pi/4)) \\
&= \frac{1}{4}\left(1 + \frac{\sqrt{2}}{2}e^{-\Delta^2}\right), \\
\mathscr{P}(|\alpha_3\rangle|\phi_3) &= \frac{1}{4}(1 - e^{-\Delta^2}\sin(7\pi/4)) \\
&= \frac{1}{4}\left(1 + \frac{\sqrt{2}}{2}e^{-\Delta^2}\right).
\end{aligned} \tag{8}$$

Therefore, the transmission probability can be defined as $\mathscr{P}_{ii} = \mathscr{P}(|\alpha_i\rangle|\phi_i)$ with $i \in \{0, 1, 2, 3\}$, which satisfies the constraint $\sum_{j=0}^{3}\mathscr{P}\left(|\alpha_i\rangle\middle|\phi_j\right) = 1$. Moreover, the transition probability can be expressed as $\mathscr{P}_{ij} = 1 - \mathscr{P}_{ii}$ with $i \neq j$. Subsequently, the QBER for Eve can be calculated as $QBER = \sum_n \mathscr{Q}_n \mathscr{R}_n$, with the notation

$$\mathscr{Q}_n = \begin{cases} \sum_{k=(n+1)/2}^{n} \mathrm{C}_n^k \mathscr{P}_{ij}^k \left(1 - \mathscr{P}_{ij}\right)^{n-k} & n \text{ is odd}, \\ \sum_{k=(n+2)/2}^{n} \mathrm{C}_n^k \mathscr{P}_{ij}^k \left(1 - \mathscr{P}_{ij}\right)^{n-k} + \frac{1}{2}\mathrm{C}_n^{n/2} \mathscr{P}_{ij}^{n/2}\left(1 - \mathscr{P}_{ij}\right)^{n/2} & n \text{ is even}, \end{cases} \tag{9}$$

and $\mathscr{R}_n = \frac{e^{-N_c} \cdot N_c^n}{n!}$, $C_n^k = \frac{n!}{k!(n-k)!}$, $n! = 1 \times 2 \times 3 \times \cdots (n-1) \times n$. Here, n and N_c symbolize the transmitted photons (at the Alice's side) and detected photons (at the Eve's side) per pulse, respectively. Figure 6a depicts the QBER for Eve with the discrete modulation protocol. Considering the existence of noise in the channel, two parameters are restricted with $n > N_c$. According to the result, we can see that, increasing the number of n and N_c will improve the QBER of the intercept-resend attack for Eve.

In the following, we analyze the performance of the Bayesian estimator for the Gaussian-modulated self-reference CVQKD protocol. The Bayesian cost can be defined by the relation

$$\overline{\mathscr{B}}(\mathbf{n}) = \int_{\phi^{'}-\pi}^{\phi^{'}+\pi} (\phi^{'} - \phi)^2 \mathscr{P}(\phi|\mathbf{n})\, \mathrm{d}\phi. \tag{10}$$

Particularly, if a suitable initial phase value $\phi^{'}$ is given, the minimum mean squared error (MMSE) estimator of $\phi^{'}$ has the form

$$\mathrm{MMSE} = \int_{\phi^{'}-\pi}^{\phi^{'}+\pi} \phi \mathscr{P}(\phi|\mathbf{n})\, \mathrm{d}\phi, \tag{11}$$

where $\phi^{'}$ can be initialized with the maximum likelihood (ML) estimate, and it can be defined as

$$\mathrm{e}^{i\phi^{'}} = \frac{1}{\hat{V}}\left[\frac{n_3 - n_4}{n_3 + n_4} + i\frac{n_5 - n_6}{n_5 + n_6}\right]. \tag{12}$$

Figure 6b simulates the performance of the different phase estimation schemes, in particular, the input intensity $\bar{n}_{\mathrm{in}}$ is simulated for the fixed phase shift $\frac{\pi}{3}$. Specifically, the blue line denotes the NFM estimator[51,53,54]. Consequently, the Bayesian estimator outperforms NFM estimator.

Although the intercept-resend attack can compromise the practical security of QKD, the two remote participants can discover eavesdropping by the following method. At the receiver, Bob randomly chooses the same number of quantum pulses and reference pulses as training signals[55]. By utilizing the training signals, we can estimate the phase compensation error on reference signals and quantum signals, respectively. If the phase compensation error on signal pulses is different from that on reference pulses, we can conclude that Eve's attack is attached in the quantum channel.

Conclusion

In this paper, we analyze a security vulnerability of strong reference pulses in the realistic self-reference CVQKD system. In this scenario, before the beam splitter attack, Eve intercepts the reference pulses emitted by Alice, and utilizing the Bayesian algorithm to estimate phase drifts of reference pulses. After phase estimation and compensation, she resubmits another reference pulses to Bob. The algorithm not only can obtain a well-motivated confidence interval, but also has robustness to noise. Thus, due to the intercept-resend attack and the beam splitter attack, Eve can bias the excess noise. Consequently, it shows that the practical security of the proposed attack can be compromised by transmitting the reference pulses in the continuous-variable quantum key distribution protocol.

Appendix

In the following, we take the four-state self-reference CVQKD protocol as an example, to derive the expression of the secret key rate under the intercept-resend attack. Assuming that the phase noise of quantum channel is zero-mean with variance V_{ch}, while the phase noise reduced by Eve's Bayesian algorithm is zero-mean with variance V_{Bayes}, the deviation of the actual phase compensation error can be given by $V_s = V_{\mathrm{ch}} - V_{\mathrm{Bayes}}$. According to the imperfect phase compensation, the actual transmittance can be defined as $T_\kappa = \kappa T$, where κ represents the phase estimation accuracy with $\kappa = \left(1 - \frac{1}{2}V_s\right)^2$, and T is the transmission efficiency. Besides, the actual excess noise can be expressed as $\epsilon_\kappa = [\epsilon + (1 - \kappa)(V - 1)]/\kappa$. Therefore, the total noise referred to the channel input can be expressed as $\chi_{\mathrm{tot}}^{\ \kappa} = \chi_{\mathrm{line}}^{\ \kappa} + \chi_{\mathrm{hom}}/T_\kappa$, with the notation $\chi_{\mathrm{line}} = 1/T_\kappa + \epsilon_\kappa - 1$.

When Alice and Bob use reverse reconciliation, the secret key rate can be defined as

$$S = \beta I(A\colon B) - \chi(B\colon E), \tag{13}$$

where β is the reconciliation efficiency, $I(A\colon B)$ is the mutual information between Alice and Bob, and $\chi(B\colon E)$ is the mutual information between Bob and Eve. Specifically, the mutual information $I(A\colon B)$ is given by[55]

$$I(A\colon B) = \frac{1}{2}\log_2\frac{V + \chi_{\mathrm{tot}}^{\ \kappa}}{1 + \chi_{\mathrm{tot}}^{\ \kappa}}. \tag{14}$$

The Holevo bound of the information between Eve and Bob is given by

$$\chi(B\colon E) = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{15}$$

where $G(x) = (x + 1)\log_2(x + 1) - x\log_2 x$. The symplectic eigenvalues $\lambda_{1,2}$ are given by

$$\lambda_{1,2} = \sqrt{\frac{1}{2}(A \pm \sqrt{A^2 - 4B})}, \tag{16}$$

where

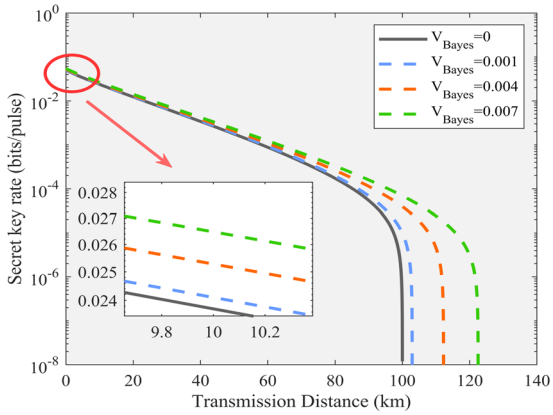


Figure 7. The theoretical and practical secret key rate of the four-state self-reference CVQKD under the intercept-resend attack. The phase noise reduced by Eve's Bayesian algorithm submits to the normal distribution with variance 0.001, 0.004 and 0.007 (rad^2) respectively. In particular, $V_{\text{Bayes}} = 0$ represents the original CVQKD protocol without the intercept-resend. Other parameters are summarized below: $\alpha = 0.35, \nu_{\text{el}} = 0.001$, $\epsilon = 0.01, \eta = 0.6, \beta = 0.95$ and $V_{\text{ch}} = 0.01(\text{rad}^2)$.

$$\begin{aligned} A &= V^2 + T_\kappa^2(V + \chi_{\text{line}}^{\kappa\ 2} - 2T_\kappa Z_4^2), \\ B &= (T_\kappa V^2 + T_\kappa V \chi_{\text{line}}^{\kappa} - T_\kappa Z_4^2)^2. \end{aligned} \tag{17}$$

The symplectic eigenvalues $\lambda_{3,4}$ are given by

$$\lambda_{3,4} = \sqrt{\frac{1}{2}(C \pm \sqrt{C^2 - 4D})}, \quad \lambda_5 = 1, \tag{18}$$

with the notation

$$\begin{aligned} C &= \frac{A\chi_{\text{hom}} + V\sqrt{B} + T_\kappa(V + \chi_{\text{line}}^{\kappa})}{T_\kappa(V + \chi_{\text{tot}}^{\kappa})}, \\ D &= \sqrt{B}\frac{V + \sqrt{B}\chi_{\text{hom}}}{T_\kappa(V + \chi_{\text{tot}}^{\kappa})}. \end{aligned} \tag{19}$$

Subsequently, we conduct numerical simulation using the realistic parameters. The parameters are summarized below: $\alpha = 0.35$, $\nu_{\text{el}} = 0.001$, $\epsilon = 0.01$, $\eta = 0.6$, $\beta = 0.95$ and $V_{\text{ch}} = 0.01(\text{rad}^2)$. Here, the phase noise reduced by Eve's Bayesian algorithm submits to the normal distribution with variance 0.001, 0.004 and 0.007 (rad^2) respectively. In particular, $V_{\text{Bayes}} = 0$ represents the original CVQKD protocol without the intercept-resend. Fig. 7 is the simulation result in the asymptotic scenario. According to the simulation result, we can conclude that, the estimated key rate based on the intercept-resend and Bayesian algorithm is higher than the true security key rate. Therefore, the attack is effective in the self-reference CVQKD protocol. In our manuscript, the proposed algorithm is described as follows.

Algorithm 1. Bayesian phase estimation

Input: Initial prior probability distribution $\mathcal{N}(\mu_0, \sigma_0)$, constant $\mathcal{K}_E$.

Output: the estimation of μ and σ .

$\mu = \mu_0$, $\sigma = \sigma_0$.

for $i \in 1 \longrightarrow m$ **do**

Obtain the outcome $\mathscr{E}$ from the experiment.

$(\mu, \sigma) = \text{Update}(\mathscr{E}, \mu, \sigma, \mathcal{K}_E)$.

end for

return (μ, σ).

Algorithm 2. Updating function

Input: the mean μ and standard derivation σ, measurement outcome $\mathscr{E}$, constant $\mathscr{K}_E$.
Output: the estimation of μ' and σ'.

function Update$(\mathscr{E}, \mu, \sigma, \mathscr{K}_E)$
  $\mu_a, \mu'_a, V_a, V'_a = 0$.
  for $i \in 1 \longrightarrow n$ **do**
    $x \sim \mathscr{N}(\mu, \sigma)$
    $x = x \bmod 2\pi$.
    $x' = x + \pi \bmod 2\pi$.
    $u \sim$ Uniform $(0, 1)$.
    if $\mathscr{P}(\mathscr{E}|x) \geq \mathscr{K}_E u$ **then**
      $\mu_a = \mu_a + x$.
      $V_a = V_a + x^2$.
      $V'_a = V'_a + x'^2$.
      $N_a = N_a + 1$.
    end if
  end for
  $\mu' = \mu_a / N_a$.
  $\sigma' = \min(\sqrt{(V_a - \mu_a^2)/(N_a - 1)}, \sqrt{(V'_a - \mu_a^2)/(N_a - 1)})$.
  return (μ', σ').
end function

Received: 12 July 2019; Accepted: 30 October 2019;
Published online: 03 December 2019

References

1. Bunandar, D. *et al*. Metropolitan quantum key distribution with silicon photonics. *Phys. Rev. X* **8**, 021009 (2018).
2. Lo, H. K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **8**, 595–604 (2015).
3. Weedbrook, C. *et al*. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621 (2012).
4. Pirandola, S. *et al*. Advances in Quantum Cryptography, arXiv:1906.01645 (2019)
5. Samuel, L. B. & Peter, V. L. Quantum information with continuous variables. *Rev. Mod. Phys.* **77**, 513 (2005).
6. Wang, S. *et al*. Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system. *Phys. Rev. X* **9**, 021046 (2019).
7. Cui, C. H. *et al*. Twin-Field Quantum Key Distribution without Phase Postselection. *Phys. Rev. Applied* **11**, 034053 (2019).
8. Wang, S. *et al*. Practical gigahertz quantum key distribution robust against channel disturbance. *Opt. Lett.* **43**, 2030–2033 (2018).
9. Wang, S. *et al*. Proof-of-principle experimental realization of a qubit-like qudit-based quantum key distribution scheme, Quantum Sci. *Technol* **3**, 025006 (2018).
10. Yin, Z. Q. *et al*. Improved security bound for the round-robin-differential-phase-shift quantum key distribution. *Nat. Commun.* **9**, 457 (2018).
11. Wang, S. *et al*. Experimental demonstration of a quantum key distribution without signal disturbance monitoring. *Nat. Photonics* **9**, 832–836 (2015).
12. Wang, S., Chen, W., Yin, Z. Q., Li, H. W. & Han, Z. F. Field and long-term demonstration of a wide area quantum key distribution network. *Opt. Express* **22**, 21739–21756 (2014).
13. Liao, S. *et al*. Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47 (2017).
14. García-Patrón, R. & Cerf, N. J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **97**, 190503 (2006).
15. Lance, A. M., Symul, T. & Sharma, V. No-switching quantum key distribution using broadband modulated coherent light. *Phys. Rev. Lett.* **95**, 180503 (2005).
16. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
17. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
18. Huang, D., Huang, P., Lin, D. & Zeng, G. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* **6**, 19201 (2016).
19. Wang, C. *et al*. 25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel. *Sci. Rep.* **5**, 14607 (2015).
20. Huang, D., Lin, D., Wang, C., Liu, W. & Zeng, G. Continuous-variable quantum key distribution with 1 Mbps secure key rate. *Opt. Express* **23**, 17511 (2015).
21. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **7**, 378–381 (2013).
22. Navascués, M., Grosshans, F. & Acín, A. Optimality of gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **97**, 190502 (2006).
23. Renner, R. & Cirac, J. I. A definetti representation theorem for infinite dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.* **102**, 110504 (2009).

24. Leverrier, A., Grosshans, F. & Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **81**, 062343 (2010).
25. Leverrier, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **114**, 070501 (2015).
26. Qian, Y. J. *et al*. Hacking the Quantum Key Distribution System by Exploiting the Avalanche-Transition Region of Single-Photon Detectors. *Phys. Rev. Applied* **10**, 064062 (2018).
27. Huang, J. Z. *et al*. Quantum hacking on quantum key distribution using homodyne detection. *Phys. Rev. A* **89**, 032304 (2014).
28. Huang, J. Z. *et al*. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A* **87**, 062329 (2013).
29. Li, H. W. *et al*. Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. *Phys. Rev. A* **84**, 062308 (2011).
30. Ma, X., Sun, S., Jiang, M. & Liang, L. Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems. *Phys. Rev. A* **88**, 022339 (2013).
31. Jouguet, P., Kunz-Jacques, S. & Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A* **87**, 062313 (2013).
32. Qin, H., Kumar, R. & Alléaume, R. Saturation Attack On Continuous-Variable Quantum Key Distribution System. *Proc SPIE* **8899**, 88990N (2013).
33. Ma, X. C., Sun, S. H., Jiang, M. S. & Liang, L. M. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. *Phys. Rev. A* **87**, 052309 (2014).
34. Huang, D., Huang, P., Lin, D., Wang, C. & Zeng, G. High-speed continuous-variable quantum key distribution without sending a local oscillator. *Opt. Lett.* **40**, 3695–3698 (2015).
35. Soh, D. B. S. *et al*. Self-referenced continuous-variable quantum key distribution protocol. *Phys. Rev. X* **5**, 041010 (2015).
36. Marie, A. & Romain, A. Self-coherent phase reference sharing for continuous-variable quantum key distribution. *Phys. Rev. A* **95**, 012316 (2017).
37. Qin, H., Kumar, R. & Alleaume, R. Quantum hacking on a practical continuous-variable quantum cryptosystem by inserting an external light, Proceedings Volume 9648, Electro-Optical and Infrared Systems: Technology and Applications XII and Quantum Information Science and Technology (2015).
38. Kunz-Jacques, S. & Jouguet, P. Robust shot-noise measurement for continuous-variable quantum key distribution. *Phys. Rev. A* **91**, 022307 (2015).
39. Ren, S. *et al*. Reference pulse attack on continuous-variable quantum key distribution with local local oscillator. *J. Opt. Soc. Am. B* **36**, 7–15 (2019).
40. Pereira, J. & Pirandola, S. Hacking Alice's box in continuous-variable quantum key distribution. *Phys. Rev. A* **98**, 062319 (2018).
41. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
42. Zhang, H., Fang, J. & He, G. Improving the performance of the four-state continuous-variable quantum key distribution by using optical amplifiers. *Phys. Rev. A* **86**, 022338 (2012).
43. Papanastasiou, P., Lupo, C., Weedbrook, C. & Pirandola, S. Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal loss channels. *Phys. Rev. A* **98**, 012340 (2018).
44. Ghorai, S., Grangier, P., Diamanti, E. & Leverrier, A. Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation. *Phys. Rev. X* **9**, 021059 (2019).
45. Wiebe, N. & Granade, C. Efficient bayesian phase estimation. *Phys. Rev. Lett.* **117**, 010503 (2015).
46. Daneshgaran, F., Delgado, M. T. & Mondin, M. Improved key rates for quantum key distribution employing soft metrics using Bayesian inference with photon counting detectors. *Quantum Communications and Quantum Imaging IX* **8163**, 113–122 (2011).
47. Paesani, S. *et al*. Experimental bayesian quantum phase estimation on a silicon photonic chip. *Phys. Rev. Lett.* **118**, 100503 (2017).
48. Wiebe, N., Granade, C., Ferrie, C. & Cory, D. G. Hamiltonian learning and certication using quantum resources. *Phys. Rev. Lett.* **112**, 190501 (2014).
49. Řeháček, J., Hradil, Z., Dušek, M., Haderka, O. & Hendrych, M. Testing operational phase concepts in quantum optics. *Quant. Semiclass. Opt* **2**, 237–244 (2000).
50. Walls, D., Milburn, G.Quantum Optics, 1st Edition, Springer, Berlin (1994).
51. Noh, J. W., Fougères, A. & Mandel, L. Measurement of the quantum phase by photon counting. *Phys. Rev. Lett.* **67**, 1426–1429 (1991).
52. Rimmer, D. & Fitzgerald, W. J. Bayesian estimation of quantum optical phase by photon counting. *Signal Process.* **84**, 1461–1471 (2004).
53. Noh, J. W., Fougères, A. & Mandel, L. Operational approach to the phase of a quantum field. *Phys. Rev. A* **45**, 424–442 (1992).
54. Řeháček, J., Hradil, Z., Dusek, M., Haderka, O. & Hendrych, M. Testing operational phase concepts in quantum optics. *J. Opt. B: Quantum Semiclass. Opt* **2**, 237–244 (1999).
55. Huang, B., Huang, Y. & Peng, Z. Practical security of the continuous-variable quantum key distribution with real local oscillators under phase attack. *Opt. Express* **27**, 20621–20631 (2019).

Acknowledgements

This work is supported by the National Nature Science Foundation of China (Grant Nos. 61801522, 61872390), and National Nature Science Foundation of Hunan Province, China (Grant No. 2019JJ40352).

Author contributions

D.H. defined the scientific goals and conceived the project. W.Z. carried out the whole protocol. R.-H.S. developed the phase estimation algorithm. W.Z., R.-H.S. and D.H. wrote the manuscript.

Competing interests

The authors declare that they have no competing interests.

Additional information

Correspondence and requests for materials should be addressed to D.H.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.