

Security Loophole Induced by Photorefractive Effect in Continuous-variable Quantum Key Distribution System

Zehao Zhou,¹ Peng Huang,^{1,2,3,*} Tao Wang,^{1,2,3} and Guihua Zeng^{1,2,3,4,†}

¹*State Key Laboratory of Advanced Optical Communication Systems and Networks,
Institute for Quantum Sensing and Information Processing,
Shanghai Jiao Tong University, Shanghai 200240, China*

²*Shanghai Research Center for Quantum Sciences, Shanghai 201315, China*

³*Hefei National Laboratory, Hefei 230088, China*

⁴*Shanghai XunTai Quantech Co., Ltd, Shanghai, 200241, China*

(Dated: September 4, 2024)

Modulators based on the Mach-Zehnder interferometer (MZI) structure are widely used in continuous-variable quantum key distribution (CVQKD) systems. MZI-based variable optical attenuator (VOA) and amplitude modulator can reshape the waveform and control the intensity of coherent state signal to realize secret key information modulation in CVQKD system. However, these devices are not ideal, internal and external effects like non-linear effect and temperature may degrade their performance. In this paper, we analyzed the security loophole of CVQKD under the photorefractive effect (PE), which originates from the crystal characteristic of lithium niobate (LN). It is found that the refractive index change of modulators because of PE may lead to an overestimate or underestimate of the final secret key rate. This allows Eve to perform further attacks like intercept-resend to get more secret key information. To solve this problem, several countermeasures are proposed, which can effectively eliminate potential risks.

I. INTRODUCTION

Quantum communication technologies is a fast-developing field that is continuously increasing in significance. Quantum key distribution (QKD) is one of the most widely researched techniques in quantum communication [1–4]. QKD systems modulate the key information on different types of quantum signals including single photons and the quadrature of quantum beam, respectively called discrete-variable QKD and continuous-variable QKD [5–11]. Compared to discrete-variable QKD (DVQKD), continuous-variable QKD (CVQKD) has apparent superiority in information transfer efficiency and implementation difficulty [12, 13]. A large proportion of CVQKD research and implementation nowadays is based on Gaussian-modulated coherent states (GMCS) schemes. Through researchers' protracted and unremitting efforts, the theoretical security of GMCS-CVQKD under individual, collective, and coherent attacks has been proven [9–11, 14–19]. GMCS-CVQKD has developed to maturation and is usually preferred because of its reliability. However, in practice, security in theory cannot guarantee the absolute security of the systems. An eavesdropper can exploit the imperfection of the actual devices to carry out side-channel attacks, and further steal (part of) the secret information [20, 21]. Therefore, it is crucial to identify and solve the practical security problems.

Currently, the proposed practical security problems of CVQKD have three orientations, respectively aiming at

the transmitting end [22–25], local oscillator light [26–28], and receiving end [29–32]. All of these attacks have corresponding defense methods put forward as well. Particularly, researchers bring forward a Local LO (LLO) scheme [33, 34] that generates LO at the receiving end directly. LLO scheme avoids the channel transmission process of LO and completely eliminates the security problems aiming at the transmitted local oscillator (LO) light. For the security problems aimed at the receiving end, researchers also established a measurement-device-independent (MDI) scheme that can defend all side-channel attacks against the detector [35–37]. These innovative results remarkably contribute to the security of CVQKD which eradicates a series of loopholes. However, attacks with other targets like modulation devices are still threatening.

Mach-Zehnder interferometer is a basic optical structure commonly seen in optical devices [38]. MZI modulators especially lithium niobate ($LiNbO_3$, LN) modulators are used in optical communication on a large scale. Lithium niobate crystals have many photoelectric effects, including piezoelectric effect, electrooptical effect, nonlinear optical effect, photovoltaic effect, photoelastic effect, photorefractive effect, and so on [39]. The excellent characteristics of the electrooptical effect and nonlinear optical effect make it favored in external modulators, like variable optical attenuator (VOA), amplitude modulator (AM), and phase modulator (PM). Similarly, other features of LN may also influence the performance in both positive and negative way. The photorefractive effect is another one that extensively exists in LN materials [40–43]. It describes the phenomenon of refractive index modulation of the waveguide under light irradiation. This index change can recover under specific conditions like heating. Although characteristics of the photore-

* huang.peng@sjtu.edu.cn

† ghzeng@sjtu.edu.cn

fractive effect may be useful in the field of data storage [44], it may introduce adverse impacts on optical modulators as it's usually ignored. Recently, the security problems resulting from photorefractive effect are researched in DVQKD [45, 46]. However, the possible security loopholes under CVQKD have not been studied yet.

In this paper, the photorefractive effect in LN-based variable optical attenuators is studied. We introduce the generation mechanism and mathematical model of the photorefractive effect in CVQKD implementation. The negative impact of the photorefractive effect on modulators' transfer characteristics is explored. It is found that the transfer function of modulators deviates under different intensity of PE will lead to inaccurate signal output. Finally, security analysis and simulation results demonstrate that the secret key rate can be underestimated or overestimated by legal parties. This suggests that the photorefractive effect in amplitude modulators may create a security loophole for Eve to conceal her attacks. To eliminate the security risks caused by the photorefractive effect, we also proposed several effective countermeasures. However, in the long view, we further give some solutions to solving the problem in fundamental. In general, our work indicates an issue that was ignored regarding the devices' fundamental properties. Eavesdropper possibly gains key information and misleads the legal communication parties from this loophole. This discovery and corresponding proposed countermeasures contribute to perfecting the practical security of CVQKD systems, bringing the quantum communication techniques closer to absolute safety.

II. PRINCIPLE OF THE LOOPHOLE FROM PHOTOREFRACTIVE EFFECT

A. Mechanism of photorefractive effect

Compared with the instantaneous Kerr effect, the photorefractive effect is a time-continuing process. For electro-optical crystals, the impurities and defects can act as the donor or acceptor of electric charges. When these crystals are irradiated by uneven light, the charges (electron or hole) of impurities and defects are excited into the conduction or valence band to form charge carriers. These charge carriers then diffuse or drift due to the concentration gradient and external electric field applied. Besides, these charges may also move because of the photovoltaic effect [40–42]. Therefore, the carriers are excited, migrated, and captured. The space charge distribution will be rearranged, and generate a space charge field. This space charge field modulates and changes the refractive index of the electro-optical crystal [45–48].

For rigorous approach, the photorefractive process is described by a series of equations called Kukhtarev equation [49]. According to the band transmission model, the generation rate of electrons under light excitation is $(N_D - N_D^+)(sI + \beta)$. Here N_D is the donor density, N_D^+

is the ionized donor density, s is the optical excitation constant, I is the light intensity and β is the thermal excitation probability. The recombination rate of electrons is $\gamma_R N_D^+ \rho$, γ_R is the recombination constant and ρ is the electron density in the conduction band [43]. The first Kukhtarev equation describing the change rate of charge carrier generation is

$$\frac{\partial N_D^+}{\partial t} = (N_D - N_D^+)(sI + \beta) - \gamma_R N_D^+ \rho, \quad (1)$$

then the current density J can be expressed by the second equation

$$J = qD \nabla \rho + q\mu\rho E + pIe_c, \quad (2)$$

where D is the diffusion coefficient, μ is the electron mobility, E is the electric field including external electric field and space-charge field, p is the photovoltaic constant, e_c is a direction vector. Three terms of the equation respectively represent diffusion current density, drift current density, and photovoltaic current density.

The continuity equation is the third one describing the carrier current:

$$\frac{\partial \rho}{\partial t} = \frac{\partial N_D^+}{\partial t} + \frac{\nabla \cdot J}{q}. \quad (3)$$

The last modulation equation gives the relationship between refractive index change and space charge field E_{sc} induced by PE:

$$\Delta n(t) = -\frac{1}{2}n_0^3\gamma_{eff}r_{33}E_{sc}(t). \quad (4)$$

n_0 is the original refractive index, γ_{eff} is the effective electro-optic coefficient, r_{33} is the Pockels coefficient. As a time-continuing process, the photorefractive index change is a function of time t . Referring to Poisson's equation, the space charge field is

$$E_{sc}(t) = (E_s - E_{sc}(0))(1 - e^{-\frac{(\sigma_d + \sigma_{ph})t}{\epsilon\epsilon_0}}) + E_{sc}(0). \quad (5)$$

Assuming the space charge field induced by PE is zero at the beginning ($E_{sc}(0) = 0$), the final space charge field will be $E_{sc}(\infty) = E_s$, where E_s is the stable space charge field, or also called saturated space charge field, which is expressed by

$$E_s = \frac{\sigma_{ph}}{\sigma_d + \sigma_{ph}}E_{app} + \frac{\kappa\alpha}{\sigma_d + \sigma_{ph}}I_{ir}. \quad (6)$$

Here σ_d is the dark conductivity, σ_{ph} is the photoconductivity, κ is the Glass constant, and α is the absorption coefficient.

Therefore, the stable or saturated refractive index change $\Delta n_s(\infty)$ is

$$\Delta n_s = -\frac{1}{2}n_0^3\gamma_{eff}r_{33}\left(\frac{\sigma_{ph}}{\sigma_d + \sigma_{ph}}E_{app} + \frac{\kappa\alpha}{\sigma_d + \sigma_{ph}}I_{ir}\right). \quad (7)$$

Then, the resulting phase deviation caused by refractive index change can be calculated with effective interaction length L , and signal wavelength λ by

$$\Delta\varphi_d = \frac{2\pi}{\lambda} \Delta n_s L. \quad (8)$$

It can be seen that the refractive index change of LN is jointly influenced by the intensity of uneven irradiation light and applied electric field. And this will further influence the quantum signal, leading to the abnormal output intensity of the modulator.

B. Impact on Mach-Zehnder modulator

Variable optical attenuator is a type of Mach-Zehnder structure LN device that is widely used in optical communication systems. In the continuous-variable QKD system, VOA plays a similar role to an amplitude modulator that adjusts the output intensity of the signal by changing the relative phase between its two arms. Typically, the transfer characteristic of the Mach-Zehnder modulator (MZM) is presented in sinusoidal function. Take MXAN-LN series modulators from *iXblue Photonics* as an instance, the transfer function is expressed by

$$I_{out} = T_{mod} \cdot \frac{I_{in}}{2} [1 + \cos(\frac{\pi}{V_{\pi}} V_{DC} - \Delta\phi_0)], \quad (9)$$

where T_{mod} is the optical transmittance of the device, V_{π} is the half-wave voltage of the modulator, and ϕ_0 is the phase deviation originates from the two arms of MZI because of fabrication error due to technological imperfections.

The analysis of the mechanical model indicates that the photorefractive effect on the Mach-Zehnder structure introduces a phase deviation $\Delta\varphi_d$ on each arm. We can define the overall phase deviation of the modulator as $\Delta\varphi_p = \Delta\varphi_d(\text{arm1}) - \Delta\varphi_d(\text{arm2})$. Therefore, the transfer function of the modulator under the photorefractive effect is expressed by

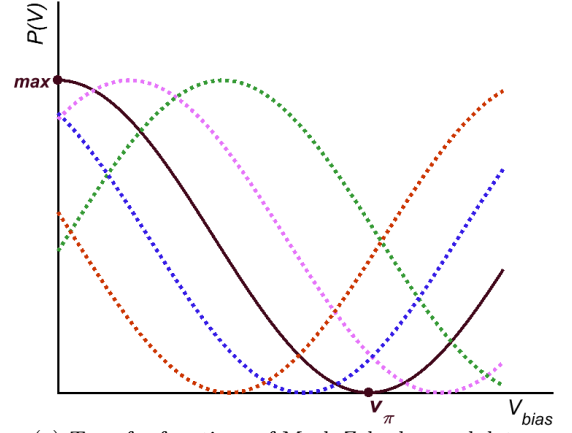
$$I'_{out} = T_{mod} \cdot \frac{I_{in}}{2} [1 + \cos(\frac{\pi}{V_{\pi}} V_{DC} - (\Delta\phi_0 + \Delta\varphi_p))]. \quad (10)$$

For further analysis, define k as an index called PE index to represent the intensity of photorefractive effect:

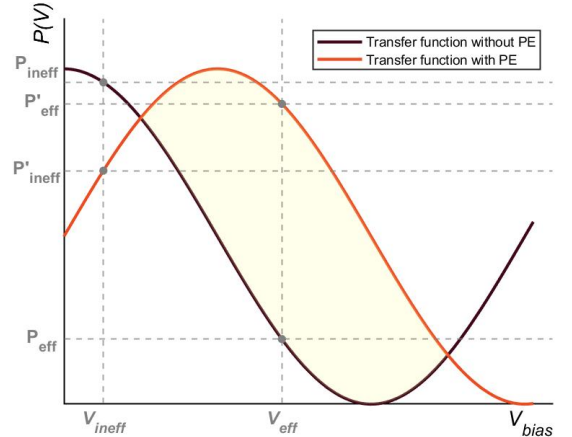
$$I'_{out} = k I_{out}. \quad (11)$$

Since the phase deviation is derived from the applied electric field and irradiation intensity, the output intensity ratio k can finally be calculated by input intensity I_{in} , applied voltage V_{DC} , and irradiation intensity I_{ir} . From Eq.(9)-Eq.(11), we can infer that

$$k = \frac{I'_{out}}{I_{out}} = \frac{1 + \cos(\frac{\pi}{V_{\pi}} V_{DC} - (\Delta\phi_0 + \Delta\varphi_p))}{1 + \cos(\frac{\pi}{V_{\pi}} V_{DC} - \Delta\phi_0)}. \quad (12)$$



(a) Transfer functions of Mach-Zehnder modulator under different applied voltage (zero at the full line)



(b) Transfer functions of modulator with and without photorefractive effect under a specific applied voltage

FIG. 1. Transfer function deviations of modulator

Substituting the Eq.(7) and Eq.(8), we know that

$$\Delta\varphi_d = \frac{e\mu\tau_0\eta_q\pi n_0^3 r_{33}\gamma I_{ir}(h\nu\kappa L - e\mu\tau_0\eta_q L_E E_{app})}{h^2\nu^2\lambda\sigma_d + h\nu e\mu\tau_0\eta_q\lambda\alpha I_{ir}}, \quad (13)$$

where the photo-conductivity is linearly dependent on irradiation intensity as $\sigma_{ph} = e\mu\tau_0\eta_q\alpha I_{ir}/h\nu$. e is the electronic charge, μ is the electron mobility, τ_0 is the carrier lifetime, η_q is the quantum efficiency, $h\nu$ is the photon energy, L_E is the waveguide length modulated by the electric field.

Therefore, the overall phase deviation $\Delta\varphi_p$ of modulator under photorefractive effect can be calculated by taking the difference of phase deviation in two arms:

$$\Delta\varphi_p = \frac{a\pi n^3 r_{33}\gamma}{\lambda_0\sigma_d} \left[L \left(\frac{I_{ir}^1}{1 + \frac{a\alpha}{\sigma_d} I_{ir}^1} - \frac{I_{ir}^2}{1 + \frac{a\alpha}{\sigma_d} I_{ir}^2} \right) - \frac{aL_E}{d} \left(\frac{I_{ir}^1}{1 + \frac{a\alpha}{\sigma_d} I_{ir}^1} + \frac{I_{ir}^2}{1 + \frac{a\alpha}{\sigma_d} I_{ir}^2} \right) V_{app} \right]. \quad (14)$$

As Eq.(14) substituting into Eq.(12), we can get the

relationship between PE index k and the controlled inputs: irradiation light intensity $I_{ir}^{1,2}$, and applied voltage V_{app} .

Research conducted in Ref.[45] revealed the characteristic change of VOA in discrete-variable QKD systems under the photorefractive effect. The photorefractive effect demonstrates identical consequences on MZM in CVQKD systems, as shown in Fig 1(a). The original transfer function of the modulator without PE is presented in full line. The power of the output signal reaches its maximum at zero bias voltage, and reaches its minimum at half-wave voltage. This conforms to Eq.(9), that the output signal intensity is the same as the input when the bias voltage is zero, as well as the output signal intensity is zero when the bias voltage is half-wave. The other dot line curves in different colors are the transfer functions under different irradiation light intensity and applied voltage. The output amplitude under PE has the same range but different at the same bias voltage. Thus, the impact of PE on MZM can be considered as the phase deviation in the transfer function.

Fig 1(b) shows the comparison of two transfer function curves respectively with (red line) and without (black line) photorefractive effect. It is apparent that under certain operating voltage like V_{eff} , the attenuation effect of the modulator can be reduced, which means $k = P''_{eff}/P_{eff} > 1$. And under some other operating voltages like V_{ineff} , the attenuation can also be strengthened, which means $k = P''_{ineff}/P_{ineff} < 1$. This is the key feature of the photorefractive effect loophole reflecting on the system. Different from the reduced optical attenuation effect proposed in Ref.[24], where k is always larger than one due to the modulator thermal damage, the photorefractive effect index can be controlled either larger or less than one. Photorefractive effect is a reversible process though it always lasts long. This benefits Eve in hiding the loophole and provides more possibilities for attack patterns.

III. PARAMETER ESTIMATION UNDER PHOTOREFRACTIVE EFFECT LOOPHOLE

A. Gaussian-modulated coherent state protocol

One-way Gaussian-modulated coherent state CVQKD system is developed to relative maturation currently [50–54]. The working process of GMCS protocol is described by the prepare-and-measure model (PM model). Firstly, communication party Alice prepares a series of quantum coherent states with two orthogonal quadratures expressed by x_i and p_i . They are modulated in Gaussian distribution with the same variance V_A and zero mean value, and are sent to the other communication party Bob through the quantum channel. Then Bob measures one or both quadratures by homodyne detection or heterodyne detection. Due to modulation shot noise, channel excess noise and transfer efficiency, results are not

completely the same as the initial states. Therefore, Bob and Alice will further share some information to perform the channel parameter estimation. The secure key rate of the system can be evaluated by estimated parameters. If the key rate is larger than zero, the communication system is secure in theory and the communication parties can finally perform data post-processing to get the final key. Otherwise, the communication will terminated and restarted.

In practice, the entanglement-based model (EB model) is always used to conduct security analysis. As shown in Fig 2, quantum coherent states prepared by Alice are equivalent to Einstein-Podolsky-Rosen (EPR) states. One mode A is kept by Alice for heterodyne detection. The other mode B_0 is sent to Bob. The variance of the vacuum state here is $V = V_A + 1$. At Bob's detection end, the practical efficiency of the detector is regarded as a beam splitter (BS) with transmittance η . And the electronic noise $e_v l$ is equivalent to the noise of an EPR state with variance v going through BS. The variance is chosen to a value that does not change the total system noise.

B. Process of parameter estimation

In the GMCS-CVQKD protocol, Alice generates a series of Gaussian-modulated coherent states. It can be expressed as:

$$|\alpha_A\rangle = |ae^{i\theta}\rangle = |x_A + ip_A\rangle. \quad (15)$$

The quadrature $x_A = |a|\cos\theta$ and $p_A = |a|\sin\theta$. Both quadratures have a variance of V_A and zero mean. It is obvious that $|a|^2$ is proportional to I_A , and $V_A = 2\langle n \rangle$ proportional to I_A as well. Therefore, the relationship between the quadratures and variance with and without photorefractive effect is

$$x'_{Ao} = \sqrt{k}x_{Ao}, \quad (16)$$

$$p'_{Ao} = \sqrt{k}p_{Ao}, \quad (17)$$

$$V'_{Ao} = kV_{Ao}. \quad (18)$$

In the GMCS-CVQKD protocol, the Gaussian attack has been proven to be optimal [9, 17]. In this situation, the quantum signal channel is assumed to be linear, as described by

$$x_B = tx_{Ao} + z, \quad (19)$$

where $t = \sqrt{\eta T}$ and z is the normal distributed noise component with total variance $\sigma^2 = \eta T\xi + N_0 + V_{el}$. This implies the relations of the following parameters without photorefractive effect:

$$\begin{cases} \langle x_{Ao}^2 \rangle = V_{X_{Ao}} \\ \langle x_{Ao}x_B \rangle = \sqrt{\eta T}V_{X_{Ao}} \\ \langle x_B^2 \rangle = \eta TV_{X_{Ao}} + \eta T\xi + N_0 + V_{el}, \end{cases} \quad (20)$$

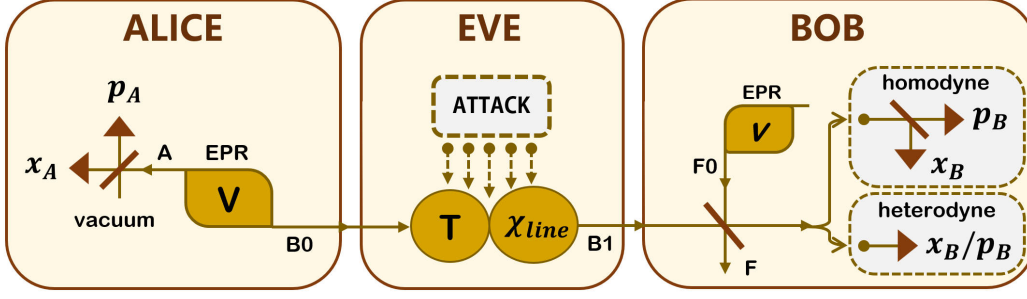


FIG. 2. Entanglement-based model of GMCS-CVQKD protocol.

x_{A_o} and x_B here represent the estimated parameters' value by Alice and Bob. Furthermore, the relationship still makes sense under a photorefractive attack. Therefore,

$$\begin{cases} \langle x'_{A_o}{}^2 \rangle = V'_{X_{A_o}} \\ \langle x'_{A_o} x'_B \rangle = \sqrt{\eta T} V'_{X_{A_o}} \\ \langle x'_B{}^2 \rangle = \eta T V'_{X_{A_o}} + \eta T \xi + N_0 + V_{el}. \end{cases} \quad (21)$$

Here, x'_{A_o} , x'_B and $V'_{X_{A_o}}$ are practical values of parameters in the operating CVQKD system. However, for the evaluation of parameters, legal parties may not realize the attack and still use x_{A_o} as they think, the relation becomes

$$\begin{cases} \langle x_{A_o}^2 \rangle = V_{X_{A_o}} \\ \langle x_{A_o} x_B \rangle = \sqrt{\eta T} V_{X_{A_o}} \\ \langle x'_B{}^2 \rangle = \eta T V_{X_{A_o}} + \eta T \xi + N_0 + V_{el}. \end{cases} \quad (22)$$

Therefore, we have

$$\sqrt{k\eta T} \mathbf{V} x_{A_o} = \sqrt{\eta T'} \mathbf{V} x_{A_o}, \quad (23)$$

and

$$k\eta T \mathbf{V} x_{A_o} + \eta T \xi = \eta T' \mathbf{V} x_{A_o} + \eta T' \xi', \quad (24)$$

which yields

$$\begin{cases} T' = kT \\ \xi' = \frac{\xi}{k} \quad (\varepsilon' = \frac{\varepsilon}{k}). \end{cases} \quad (25)$$

Therefore, the practical transmittance of a one-way GMCS-CVQKD system under photorefractive effect is k times of the transmittance without PE. While the excess noise with PE is one- k^{th} of that without PE.

IV. SECURITY ANALYSIS AND KEY RATE UNDER PHOTOREFRACTIVE EFFECT

The security analysis and secret key rate (SKR) calculation is implemented referring entanglement-based

model as well. The security proof of one protocol is in fact proceeded by secret key rate calculation under specific attacks. Since collective attacks have been proven to be the most powerful attack in asymptotic conditions [17–19], a system can be considered as secure if the secure key rate is larger than zero under collective attacks. Specifically, in the case of reverse reconciliation, the secure key rate can be written as

$$R = f \cdot (\beta I_{AB} - \chi_{BE}), \quad (26)$$

where f is the repetition frequency of signal pulses, $\beta \in (0, 1)$ is the reverse reconciliation efficiency, I_{AB} is the mutual information between Alice and Bob, and χ_{BE} is the maximum amount of information that Eve can extract from Bob's key. Without loss of generality, the following analysis of security mainly concentrates on homodyne detection.

For I_{AB} , under homodyne detection, it can be calculated by Shannon's equation with measurement variance and the conditional variance of Bob [55] as

$$I_{AB} = \frac{1}{2} \log_2 \frac{V_B}{V_{B|A}} = \frac{1}{2} \log_2 \frac{V + \chi_{tot}}{1 + \chi_{tot}}, \quad (27)$$

where $V_B = \eta T(V + \chi_{tot})$ and $V_{B|A} = \eta T(1 + \chi_{tot})$, χ_{tot} is the total noise referring to the channel input, it can be expressed as $\chi_{tot} = \chi_{line} + \chi_{hom}/T$. The total channel-added noise is further defined as $\chi_{line} = (1 + T\epsilon)/T - 1 = 1/T + \epsilon - 1$. For the detection-added noise referring to Bob's input χ_{hom} can be calculated respectively as

$$\chi_{hom} = [(1 - \eta) + v_{el}]/\eta, \quad (28)$$

where η is the equivalent BS efficiency modeled by the EB model mentioned before, and v_{el} is the electronic noise of the detector.

Then, estimating the upper bound of the information χ_{BE} that Eve can obtain is the core of secret key calculation. Under collective attacks, the Holevo bound is applied to estimate the maximum information Eve can extract [17, 18, 56, 57], which can be acquired by

$$\chi_{BE} = \sum_{i=1}^2 G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^5 G\left(\frac{\lambda_i - 1}{2}\right), \quad (29)$$

here $G(x) = (x + 1) \log_2(x + 1) - x \log_2 x$ is the von Neumann entropy function.

The covariance matrix γ_{AB_1} for the state ρ_{AB_1} corresponds to the eigenvalues $\lambda_{1,2}$, while the covariance matrix γ_{AB_1} for the state $\rho_{AB_1}^{m_B}$ corresponds to the eigenvalues $\lambda_{3,4,5}$. The symplectic eigenvalues λ_1 and λ_2 can be calculated as

$$\lambda_{1,2} = \frac{1}{2} \left(A \pm \sqrt{A^2 - 4B} \right), \quad (30)$$

where

$$A = V^2(1 - 2T) + 2T + T^2(V + \chi_{\text{line}})^2, \quad (31)$$

$$B = T^2(V\chi_{\text{line}} + 1)^2. \quad (32)$$

Similarly, analyzing the matrix $\gamma_{AFG}^{m_B}$, eigenvalues λ_3 and λ_4 can be calculated as follows: $\gamma_{AFG}^{m_B}$. The eigenvalues are calculated as:

$$\lambda_{3,4} = \frac{1}{2} \left(C \pm \sqrt{C^2 - 4D} \right), \quad (33)$$

where

$$C_{\text{hom}} = \frac{A\chi_{\text{hom}} + V\sqrt{B} + T(V + \chi_{\text{line}})}{T(V + \chi_{\text{tot}})}, \quad (34)$$

$$D_{\text{hom}} = \frac{\sqrt{B}V + \sqrt{B}\chi_{\text{hom}}}{T(V + \chi_{\text{tot}})}. \quad (35)$$

Therefore, the final secure key rate of the system can be calculated by modulation variance V_A , transmittance T , excess noise ϵ , detection efficiency η , and electric noise v_{el} . The final key rate is a function related to these parameters and so we can get a law that

- The practical security key rate without light injection attack K is calculated by: $V_A, T, \epsilon, \eta, v_{el}$
- The practical security key rate with light injection attack K_p is calculated by: $V'_A, T, \epsilon, \eta, v_{el}$
- The estimated security key rate with light injection attack K_e evaluated by Alice and Bob is calculated by: $V_A, T', \epsilon', \eta, v_{el}$

The brown and red surfaces are respectively the practical secret key rate and estimated secret key rate under a range of transmittance and PE index. Two surfaces intersect at the yellow dot line, where the PE index is 1. It is obvious that the practical SKR will be the same as the estimated SKR in this situation. When $k < 1$, it can be seen that the practical SKR is always smaller than the estimated SKR. In this situation, the performance of the system is degraded. When $k > 1$, the practical SKR is always larger than the estimated SKR. In this situation, SKR is overestimated, the estimated security key rate will be larger than the practical security key rate at the same distance. As well as Alice and Bob will underestimate the excess noise of the system, which means the estimated excess noise will be larger than the practical one.

This creates a space for Eve allowing her to introduce additional excess noise to the system. Therefore, a security loophole is created that she can implement extra attacks like intercept-resend attacks to get the key information. Besides, it can be found that as k becomes larger, the difference between practical SKR and estimated SKR gets larger too. This reflects that the leaking of the secret key information increases with a higher PE index. According to the above analysis, the optimal choice for Eve is to control the intensity of the photorefractive effect to keep the PE index larger than one ($k > 1$). This also requires the bias voltage calibrated by users to be with the yellow region in Fig 1.

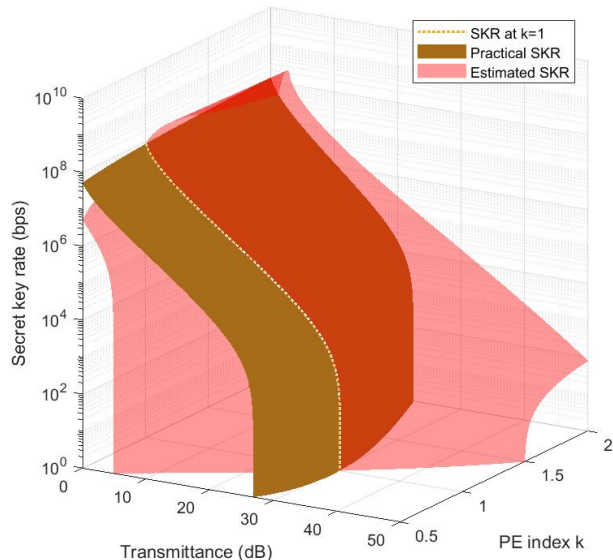


FIG. 3. Practical and estimated secret key rate versus transmittance and PE index with 0.2 dB/km fiber loss, $f = 300\text{MHz}$, $\eta = 0.6$, $v_{el} = 0.01$, $\epsilon = 0.05$, $V_A = 4$, $\beta = 0.95$.

Furthermore, Fig 4 shows the simulation results of secret key rate under different excess noise, respectively at $k = 0.8$ and $k = 1.2$. Both of the results indicate that the gap between practical and estimated SKR becomes bigger under the same PE index, as the excess noise becomes larger. This demonstrates that in the case of a larger excess noise, when $k < 1$, Eve can degrade the communication performance to a greater extent; when $k > 1$, Eve can acquire more secret key information.

V. COUNTERMEASURES

A. Attack pattern

Through the security analysis, it is found that the photorefractive effect that occurs on the modulator will open a security loophole. For Eve, there are different attack

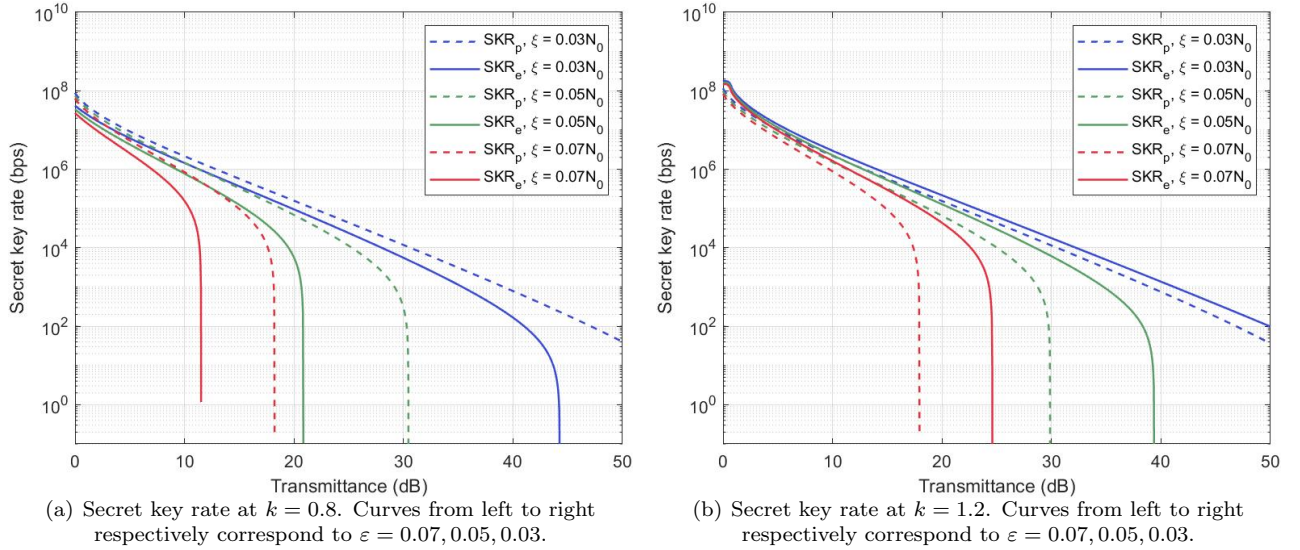


FIG. 4. Simulation results of secret key rate versus transmittance. Estimated result presented in solid line, practical result presented in dot line, parameters except excess noise keep unchanged.

patterns to control the photorefractive effect of modulators.

The first way to manipulate the modulator is to inject the light beam reversely into the modulators by coupling a laser. As shown in Fig 5, the power of irradiation light can be adjusted by modulating the laser's pulse width. Under this pattern, the intensity of the photorefractive effect (PE index, k) is determined by irradiation power. Experiments in Ref.[45] have shown that the irradiation is even effective at only $3nW$. For this reason, Eve can promise the modulator to be not damaged.

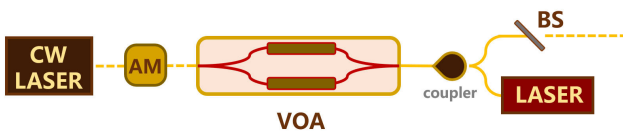


FIG. 5. System diagram of traditional attack strategy

The other way to create the loophole does not need to break the system. As mentioned, the photorefractive effect is a continuous process with a relatively long-term result. Generally, the photorefractive effect can last many weeks to several months in LN material [40–42, 47, 48]. Therefore, Eve can act as the device supplier. She then processes the MZM under a specific electric field and irradiation to cause PE. This is done before providing it to Alice and Bob. The effect remains after the CVQKD system is established, and so that the loophole will exist originally in system. This way is more simple in implementation compared to the first one.

B. Defense strategy

Corresponding to the possible attack patterns, we also put forward some countermeasures. To fill the loophole, the direct solution is adding isolators or circulators after the modulator. However, the effect of isolation can still be weakened or destroyed under high reverse power. Besides, the real-time monitoring scheme can also have an effect. By monitoring the variation of the modulation variance in real-time, Alice and Bob can evaluate the PE index k at any time. Therefore they can correct the parameters and get the proper secret key rate. Since the consequence of the PE loophole is similar to the reduced attenuation effect, the monitoring system can be designed referring to that in Ref.[24] as well.

For the second pattern, the direct solution is to calibrate the modulators before putting them into service. However, this cannot fill the loophole perfectly as well. As time goes by, the recovery of the photorefractive effect will lead to the transfer function deviations again. The security loophole will reappear. Similar to the real-time monitoring system, it is effective to adjust the operating state of modulators in real-time. Therefore, users can promise the modulators are always in calibration. Currently, there is a mature product provided for automatic bias control (eg. iXblue MBC-DG-LAB). These controllers allow users to lock the operating point of LN Mach-Zehnder modulators, and to ensure a stable operation over time and environmental conditions [58]. It is suggested to use the modulators jointly with this kind of automatic bias controller.

In long-term consideration, addressing the loophole in fundamental is preferred rather than just filling the loophole. The ultimate countermeasure is to eliminate the photorefractive effect. Optical cleaning is a way proposed

in Ref.[59]. When the LN crystal is raised at approximately 180°C , the light beam is able to excite ions to transfer outside the illuminated region. Then these ions compensate the electronic space-charge field and the illuminated region is cleared. This can significantly enhance the resistance to PE.

Besides, the large amount of intrinsic defect due to the lack of lithium or non-stoichiometric structure of LN crystal is the fundamental reason for the photorefractive effect [60, 61]. Therefore, doping other elements in LN can also enhance the resistivity to PE. Until now, research has shown that the doping of magnesium, zinc, scandium, indium, hafnium, zirconium, and stannum can all inhibit the photorefractive effect [62, 63]. Especially *Mg* doped LN and *Zr* doped LN have high PE resistance and high crystalline quality. In view of this, the manufacturers are supposed to produce the modulators with doped LN devices in the future to completely close this PE security loophole.

VI. CONCLUSION

In this paper, we explore the photorefractive effect of LN crystals. Specifically, we studied the model of the effect and found its impact on LN-based Mach-Zehnder modulators. The transfer function of the amplitude mod-

ulator is deviated in phase. The intensity of PE k is various and this related to the parameter estimation of the one-way GMCS-CVQKD system. The results of security analysis show that the secret key rate is overestimated by Alice and Bob, so that a security loophole is created when $k > 1$. Eve is able to utilize the loophole to get the key information by intercept-resend attack. The leakage of key information is greater with larger system excess noise. Other than proposing the PE security loophole, we also put forward countermeasures against it. Communication parties can directly use isolators and calibrate modulators, or apply the variance real-time monitoring and automatic bias controller. However, in the future, this security loophole may be closed by optical cleaning techniques and using doped-LN Mach-Zehnder modulators.

VII. ACKNOWLEDGMENTS

This work was supported by the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300703), Shanghai Municipal Science and Technology Major Project (2019SHZDZX01), the Key R&D Program of Guangdong province (Grant No. 2020B0303040002), and the National Natural Science Foundation of China (No. 62101320).

-
- [1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theoretical Computer Science* **560**, 7 (2014), *theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84*.
 - [2] A. K. Ekert, Quantum cryptography based on bell’s theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [3] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science* **283** 5410, 2050 (1998).
 - [4] P. W. Shor and J. Preskill, Simple proof of security of the bb84 quantum key distribution protocol, *Phys. Rev. Lett.* **85**, 441 (2000).
 - [5] T. C. Ralph, Continuous variable quantum cryptography, *Phys. Rev. A* **61**, 010303 (1999).
 - [6] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Quantum cryptography without switching, *Phys. Rev. Lett.* **93**, 170504 (2004).
 - [7] M. Hillery, Quantum cryptography with squeezed states, *Phys. Rev. A* **61**, 022309 (2000).
 - [8] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, Generalized privacy amplification, *IEEE Transactions on Information Theory* **41**, 1915 (1995).
 - [9] R. García-Patrón and N. J. Cerf, Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution, *Phys. Rev. Lett.* **97**, 190503 (2006).
 - [10] A. Leverrier, Composable security proof for continuous-variable quantum key distribution with coherent states, *Phys. Rev. Lett.* **114**, 070501 (2015).
 - [11] A. Leverrier, Security of continuous-variable quantum key distribution via a gaussian de finetti reduction, *Physical Review Letters* **118**, 10.1103/physrevlett.118.200501 (2017).
 - [12] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, *Nature Communications* **8**, 10.1038/ncomms15043 (2017).
 - [13] G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, and A. Q. Liu, An integrated silicon photonic chip platform for continuous-variable quantum key distribution, *Nature Photonics* **13**, 839 (2019).
 - [14] F. Grosshans and N. J. Cerf, Continuous-variable quantum cryptography is secure against non-gaussian attacks, *Physical Review Letters* **92**, 10.1103/physrevlett.92.047905 (2004).
 - [15] F. Grosshans and P. Grangier, Continuous variable quantum cryptography using coherent states, *Phys. Rev. Lett.* **88**, 057902 (2002).
 - [16] J. Lodewyck and P. Grangier, Tight bound on the coherent-state quantum key distribution with heterodyne detection, *Physical Review A* **76**, 10.1103/physreva.76.022332 (2007).
 - [17] M. Navascués, F. Grosshans, and A. Acín, Optimality of gaussian attacks in continuous-variable quantum cryptography, *Phys. Rev. Lett.* **97**, 190502 (2006).
 - [18] M. M. Wolf, G. Giedke, and J. I. Cirac, Extremality of gaussian quantum states, *Physical Review Letters* **96**, 10.1103/physrevlett.96.080502 (2006).

- [19] F. Grosshans, Collective attacks and unconditional security in continuous variable quantum key distribution, *Physical Review Letters* **94**, 10.1103/physrevlett.94.020504 (2005).
- [20] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, Continuous-variable quantum key distribution system: Past, present, and future, *Applied Physics Reviews* **11**, 011318 (2024), https://pubs.aip.org/aip/apr/article-pdf/doi/10.1063/5.0179566/19855574/011318_1.5.0179566.pdf.
- [21] 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).
- [22] P. Huang, G. He, and G. Zeng, Bound on noise of coherent source for secure continuous-variable quantum key distribution, *International Journal of Theoretical Physics* **52** (2013).
- [23] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, Trojan-horse attacks threaten the security of practical quantum cryptography, *New Journal of Physics* **16**, 123030 (2014).
- [24] Y. Zheng, P. Huang, A. Huang, J. Peng, and G. Zeng, Practical security of continuous-variable quantum key distribution with reduced optical attenuation, *Phys. Rev. A* **100**, 012313 (2019).
- [25] Y. Zheng, P. Huang, A. Huang, J. Peng, and G. Zeng, Security analysis of practical continuous-variable quantum key distribution systems under laser seeding attack, *Opt. Express* **27**, 27369 (2019).
- [26] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, Local oscillator fluctuation opens a loophole for eavesdropping in practical continuous-variable quantum-key-distribution systems, *Phys. Rev. A* **88**, 022339 (2013).
- [27] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution, *Phys. Rev. A* **87**, 062313 (2013).
- [28] Y. Zhao, Y. Zhang, Y. Huang, B. Xu, S. Yu, and H. Guo, Polarization attack on continuous-variable quantum key distribution, *Journal of Physics B: Atomic, Molecular and Optical Physics* **52**, 015501 (2018).
- [29] H. Qin, R. Kumar, V. Makarov, and R. Alléaume, Homodyne-detector-blinding attack in continuous-variable quantum key distribution, *Phys. Rev. A* **98**, 012312 (2018).
- [30] C. Wang, P. Huang, D. Huang, D. Lin, and G. Zeng, Practical security of continuous-variable quantum key distribution with finite sampling bandwidth effects, *Phys. Rev. A* **93**, 022315 (2016).
- [31] H. Qin, R. Kumar, and R. Alléaume, Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution, *Phys. Rev. A* **94**, 012325 (2016).
- [32] J.-Z. Huang, C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack, *Phys. Rev. A* **87**, 062329 (2013).
- [33] 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* **5**, 041009 (2015).
- [34] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Self-referenced continuous-variable quantum key distribution protocol, *Phys. Rev. X* **5**, 041010 (2015).
- [35] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, Continuous-variable measurement-device-independent quantum key distribution, *Phys. Rev. A* **89**, 052301 (2014).
- [36] Y. Tian, P. Wang, J. Liu, S. Du, W. Liu, Z. Lu, X. Wang, and Y. Li, Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber, *Optica* **9**, 492 (2022).
- [37] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, High-rate measurement-device-independent quantum cryptography, *Nature Photonics* **9**, 397 (2015).
- [38] Y. Fu, X. Zhang, B. Hraimel, T. Liu, and D. Shen, Mach-zehnder: A review of bias control techniques for mach-zehnder modulators in photonic analog links, *IEEE Microwave Magazine* **14**, 102 (2013).
- [39] A. Boes, L. Chang, C. Langrock, M. Yu, M. Zhang, Q. Lin, M. Lončar, M. Fejer, J. Bowers, and A. Mitchell, Lithium niobate photonics: Unlocking the electromagnetic spectrum, *Science* **379**, eabj4396 (2023), <https://www.science.org/doi/pdf/10.1126/science.abj4396>.
- [40] J.-P. Ruske, B. Zeitner, A. Tunnermann, and A. Rasch, Photorefractive effect and high power transmission in linbo3 channel waveguides, *Electronics Letters* **39**, 1048 (2003).
- [41] G. Harvey, The photorefractive effect in directional coupler and mach-zehnder linbo/sub 3/ optical modulators at a wavelength of 1.3 μm , *Journal of Lightwave Technology* **6**, 872 (1988).
- [42] A. M. Glass, The Photorefractive Effect, *Optical Engineering* **17**, 175470 (1978).
- [43] S. M. Kostrikskii, Photorefractive effect in linbo3-based integrated-optical circuits at wavelengths of third telecom window, *Applied Physics B* **95**, 421 (2009).
- [44] K. Buse, A. Adibi, and D. Psaltis, Non-volatile holographic storage in doubly doped lithium niobate crystals, *Nature* **393**, 665 (1998).
- [45] P. Ye, W. Chen, G.-W. Zhang, F.-Y. Lu, F.-X. Wang, G.-Z. Huang, S. Wang, D.-Y. He, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Induced-photorefractive attack against quantum key distribution, *Phys. Rev. Appl.* **19**, 054052 (2023).
- [46] F.-Y. Lu, P. Ye, Z.-H. Wang, S. Wang, Z.-Q. Yin, R. Wang, X.-J. Huang, W. Chen, D.-Y. He, G.-J. Fan-Yuan, G.-C. Guo, and Z.-F. Han, Hacking measurement-device-independent quantum key distribution, *Optica* **10**, 520 (2023).
- [47] T. Hall, R. Jaura, L. Connors, and P. Foote, The photorefractive effect—a review, *Progress in Quantum Electronics* **10**, 77 (1985).
- [48] R. A. Becker and R. C. Williamson, Photorefractive effects in LiNbO3 channel waveguides: Model and experimental verification, *Applied Physics Letters* **47**, 1024 (1985), https://pubs.aip.org/aip/apl/article-pdf/47/10/1024/18455526/1024.1_online.pdf.
- [49] S. G. O. M. S. N. V. Kukhtarev, V. B. Markov and V. L. Vinetskii, Holographic storage in electrooptic crystals. i. steady state, *Ferroelectrics* **22**, 949 (1978), <https://doi.org/10.1080/00150197908239450>.
- [50] Y. Pan, H. Wang, Y. Shao, Y. Pi, Y. Li, B. Liu, W. Huang, and B. Xu, Experimental demonstration of high-rate discrete-modulated continuous-variable quan-

- tum key distribution system, *Opt. Lett.* **47**, 3307 (2022).
- [51] F. Ji, P. Huang, T. Wang, X. Jiang, and G. Zeng, Gbps key rate passive-state-preparation continuous-variable quantum key distribution within an access-network area, *Photon. Res.* **12**, 1485 (2024).
- [52] D. Huang, P. Huang, D. Lin, and G. Zeng, Long-distance continuous-variable quantum key distribution by controlling excess noise, *Scientific Reports* **6**, 19201 (2016).
- [53] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, Long-distance continuous-variable quantum key distribution over 202.81 km of fiber, *Phys. Rev. Lett.* **125**, 010502 (2020).
- [54] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, *Nature Photonics* **7**, 378 (2013).
- [55] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers, *Journal of Physics B: Atomic, Molecular and Optical Physics* **42**, 114014 (2009).
- [56] A. Leverrier, F. Grosshans, and P. Grangier, Finite-size analysis of a continuous-variable quantum key distribution, *Phys. Rev. A* **81**, 062343 (2010).
- [57] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Security of continuous-variable quantum key distribution against general attacks, *Phys. Rev. Lett.* **110**, 030502 (2013).
- [58] Y. Fu, X. Zhang, B. Hraimel, T. Liu, and D. Shen, Mach-zehnder: A review of bias control techniques for mach-zehnder modulators in photonic analog links, *IEEE Microwave Magazine* **14**, 102 (2013).
- [59] M. Kösters, B. Sturman, P. Werheit, D. Haertle, and K. Buse, Optical cleaning of congruent lithium niobate crystals, *Nature Photonics* **3**, 510 (2009).
- [60] Y. Kong, F. Bo, W. Wang, D. Zheng, H. Liu, G. Zhang, R. Rupp, and J. Xu, Recent progress in lithium niobate: Optical damage, defect simulation, and on-chip devices, *Advanced Materials* **32**, 1806452 (2019).
- [61] D. Eichmann, Lithium niobate defects photorefracton and ferroelectric switching (2016).
- [62] Y. Kong, S. Liu, and J. Xu, Recent advances in the photorefracton of doped lithium niobate crystals, *Materials* **5**, 1954 (2012).
- [63] H. Liu, X. Xie, Y. Kong, W. Yan, X. Li, L. Shi, J. Xu, and G. Zhang, Photorefractive properties of near-stoichiometric lithium niobate crystals doped with iron, *Optical Materials* **28**, 212 (2006).
- [64] F. Grosshans and P. Grangier, Continuous variable quantum cryptography using coherent states, *Phys. Rev. Lett.* **88**, 057902 (2002).
- [65] R. Renner and J. I. Cirac, de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography, *Phys. Rev. Lett.* **102**, 110504 (2009).
- [66] A. Leverrier and P. Grangier, Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation, *Phys. Rev. Lett.* **102**, 180504 (2009).
- [67] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Controlling excess noise in fiber-optics continuous-variable quantum key distribution, *Phys. Rev. A* **72**, 050303 (2005).
- [68] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, *Nature Photonics* **7**, 378–381 (2013).
- [69] J. Sudjana, L. Magnin, R. García-Patrón, and N. J. Cerf, Tight bounds on the eavesdropping of a continuous-variable quantum cryptographic protocol with no basis switching, *Physical Review A* **76**, 052301 (2007).
- [70] A. Leverrier, Security of continuous-variable quantum key distribution via a gaussian de finetti reduction, *Physical Review Letters* **118**, 10.1103/physrevlett.118.200501 (2017).