


Article

Counteracting a Saturation Attack in Continuous-Variable Quantum Key Distribution Using an Adjustable Optical Filter Embedded in Homodyne Detector

Shengjie Xu ^{1,†}, Yin Li ^{1,†}, Yun Mao ^{1,*} and Ying Guo ^{1,2,*} 

¹ School of Automation, Central South University, Changsha 410083, China; 206214@csu.edu.cn (S.X.); liyin@csu.edu.cn (Y.L.)

² School of Computer, Beijing University of Posts and Telecommunications, Beijing 100876, China

* Correspondence: maoyun3106@csu.edu.cn (Y.M.); yinggao@csu.edu.cn (Y.G.)

† These authors contributed equally to this work.

Abstract: A saturation attack can be employed for compromising the practical security of continuous-variable quantum key distribution (CVQKD). In this paper, we suggest a countermeasure approach to resisting this attack by embedding an adjustable optical filter (AOF) in the CVQKD system. Numerical simulations illustrate the effects of the AOF-enabled countermeasure on the performance in terms of the secret key rate and transmission distance. The legal participants can trace back the information that has been eavesdropped by an attacker from the imperfect receiver, which indicates that this approach can be used for defeating a saturation attack in practical quantum communications.

Keywords: continuous-variable; quantum key distribution; saturation attack; adjustable optical filter



Citation: Xu, S.; Li, Y.; Mao, Y.; Guo, Y. Counteracting a Saturation Attack in Continuous-Variable Quantum Key Distribution Using an Adjustable Optical Filter Embedded in Homodyne Detector. *Entropy* **2022**, *24*, 383. <https://doi.org/10.3390/e24030383>

Academic Editors: Vladyslav Usenko, Stefano Olivares and Marcin Jarzyna

Received: 20 January 2022

Accepted: 7 March 2022

Published: 9 March 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Quantum key distribution (QKD), which allows two legal parties, Alice and Bob, to share a set of secret key, may be manipulated by an eavesdropper, called Eve [1–5]. Currently, discrete-variable (DV) QKD has been developed, but it still faces challenges regarding the source preparation, the detection cost, and the secret key rate [6,7]. Continuous-variable (CV) QKD is another approach to actualizing QKD [8–13]. It has the advantage of convenient implementations, as it can be performed with diversification of sources such as coherent state [14] and squeezed state [15]. Nonetheless, CVQKD also faces threats of the practical security [16–18], resulting from device imperfections, technical deficiencies, and operational imperfections [10,19,20]. For example, Eve can perform a wavelength attack by controlling the transmittance of the wavelength-dependent beam splitter (BS) [21–23]. The calibration attack may be implemented by modifying the shape of the local oscillator (LO) pulse [24]. Consequently, several countermeasures have been proposed to counteract the effects of the LO calibration attack and the wavelength attacks [25–27].

In practical implementations of CVQKD, the coherent detector becomes vulnerable. Currently, the saturation attack has been performed while eavesdropping imperfect electronics in a homodyne detector [2,28]. It can be used for attacking the actual devices of the system, and thus it weakens the practical security because the coherent detector has a finite linearity domain that could be driven (if not being monitored) outside by displacing the mean value of the received quadratures. In addition, Eve may perform heterodyne detection to measure both quadratures X and P intercepted, and hence prepare for a faked coherent state [28,29]. In order to counteract such an attack, we may employ an embedded adjustable optical filter (AOF) in homodyne detectors that can be used to compensate for the potential saturation led by the strong received optical power in real time. The AOF-enabled detection, which is an actual gain adjustment of the avalanche photo-diode (APD), can be used for counteracting this saturation attack, based on the feedback of the response of detection.

This paper is organized as follows. In Section 2, we suggest an AOF-embedded CVQKD system to counteract the saturation attack. In Section 3, we perform numerical simulations to show effects of the AOF-enabled detection on the practical security of the CVQKD system. Finally, we conclude in Section 4.

2. The AOF-Embedded CVQKD

An eavesdropper can bias the excess noise estimation beyond the null key threshold by using the saturation attack, thus leading to a potential security loophole. In order to counteract this attack, an off-the-shelf detector has been employed at the receivers while performing data post-processing [28]. In this section, we consider an AOF-embedded CVQKD system that counteracts the saturation attack on-line, as shown in Figure 1a. The structure of the AOF-embedded CVQKD system is described in Appendix A. In addition, the AOF-enabled scheme is designed in Appendix B and the parameter estimation is derived in Appendix C, respectively.

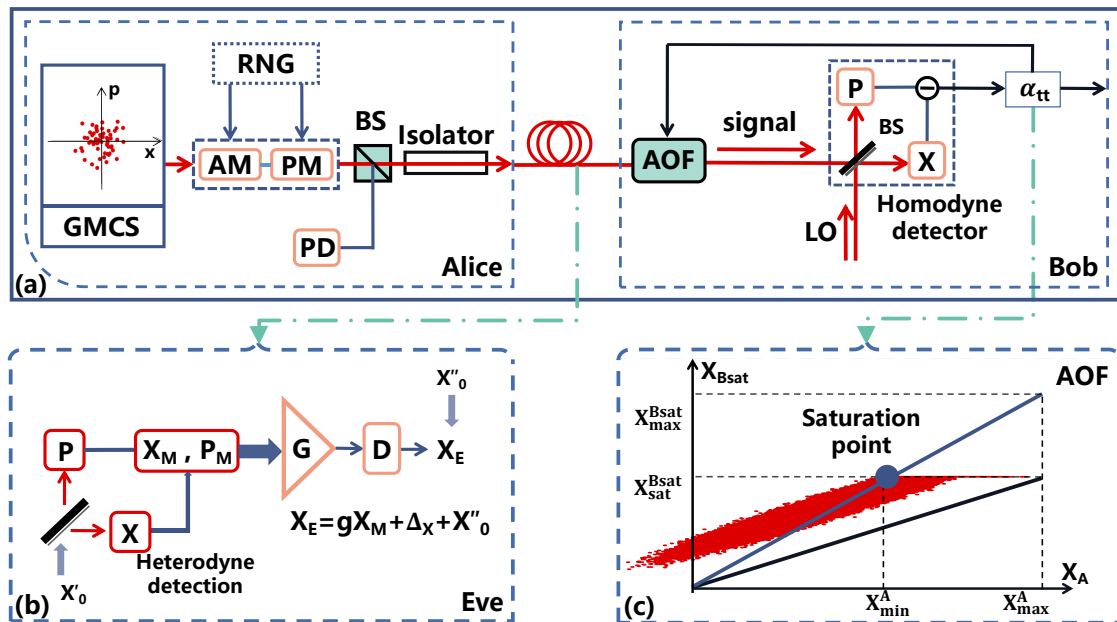


Figure 1. The AOF-embedded CVQKD. (a) System diagram: Alice prepares for coherent states with quadratures X and P ; Bob performs homodyne detection; AM, amplitude modulator; PM, phase modulator; BS, beam splitter; PD, photodetector. (b) Strategy of saturation attack on CVQKD. G , gain g ; D , displacement Δ . (c) Demonstration of operation α_{tt} for AOF.

The tunable AOF is employed for counteracting the saturation attack in CVQKD, where the data post-processing involves evaluation of attenuation (α_{tt}), which can be used for saturation compensation [28]. In Figure 1c, we illustrate the results of the saturation-involved attenuation evaluation, where abscissa X_A is prepared for Alice, the ordinate X_{Bsat} is Bob’s measurement results, and the red pots represent Eve’s measurement results. There are values of the saturation data X_{sat}^{Bsat} , the maximum data X_{max}^A , and the saturation point $(X_{smin}^A, X_{sat}^{Bsat})$, where X_{smin}^A is the minimum value sent by Alice when the measurement results are saturated. It is noted that X_{max}^{Bsat} is the value corresponding to X_{max}^A in the blue line, which is derived by connecting the saturation point with the zero point. While making the measurement results in a finite linearity domain, we regulate the initial line from the black line after attenuation. Subsequently, we obtain the relationship of the blue line and the black line given by

$$X_{max}^{Bsat} = k_1 X_{max}^A, \quad X_{sat}^{Bsat} = k_2 X_{max}^A, \tag{1}$$

with the constraint $k_2 = \alpha_{tt}k_1$, where α_{tt} is the attenuation with $\alpha_{tt} = X_{\text{sat}}^{\text{Bsat}}(X_{\text{max}}^{\text{Bsat}})^{-1}$. We note that α_{tt} is an operation that should be performed at the receiver for data-processing with measurement results.

In what follows, we perform the data-processing for the operation α_{tt} , which is an algorithm for measurement results in essence. The initial attenuation α_{tt} is assumed to be one. When the first data block is performed, the resulting attenuation α_{tt} is updated on the initial one. The AOF is then performed for attenuation on the second data block according to the feedback of the previous attenuation. After that, the second block needs to derive the attenuation value. When there is no attenuation evaluated, the data block can be used to estimate the excess noise. Otherwise, the attenuation evaluated by the second data block is updated to attenuate the following block, and it has to repeat the aforementioned procedures.

3. Security Analysis

To demonstrate the effects of the AOF-enabled counteraction approach on the performance of system, we perform the saturation attack in CVQKD, which is illustrated in Appendix B. This strategy can be implemented by regulating the displacement Δ and the gain g . The effects of a saturation attack on parameter estimation are shown in Appendix C. We take into account measurements of data block size N , which is the number of coherent states prepared by Alice. In Figure 2, we show the effects of block size N on estimated excess noise with $N \in \{10^6, 10^7, 10^8\}$. We find that the large block size N may result in small excess noise. Without loss of generality, we consider numerical simulations of the AOF-embedded CVQKD system for $N = 10^7$. In this section, all of the excess noises in numerical simulations are described in terms of shot-noise units.

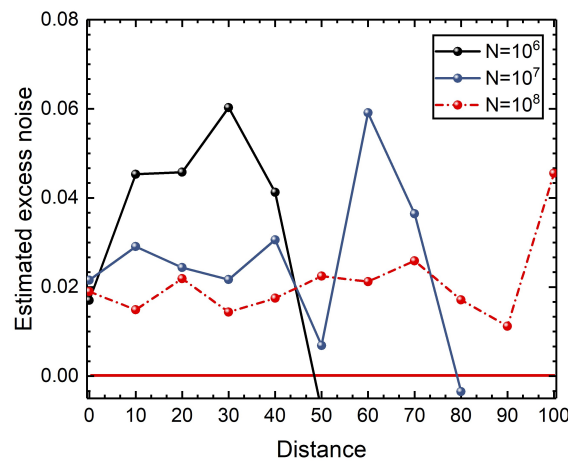


Figure 2. Effects of block size N on the estimated excess noise. The excess noise in numerical simulations are described in terms of shot-noise units.

3.1. Effects on Excess Noise

In Figure 3, we show measurement results under the saturation attack, where red dots, blue dots, and light dots denote measurement results for the saturation attack, the infinite linearity domain, and the attenuation, respectively. Due to the saturation attack, Alice and Bob may achieve the counterfeited information. However, as eavesdropping may increase the excess noise that make the generation of a secret key forbidden, Alice and Bob can detect the saturation attack in the traditional system, where the secret key rate may be decreased. In order to illustrate the effect of the AOF-enabled counteraction on the excess noise, we consider effects of the parameter displacement Δx on the attacked CVQKD system. As shown in Figure 4, after performing the AOF-enabled counteraction scheme, the estimated excess noises fall in the finite linearity domain, which can lead to the performance improvement in terms of secret key rate.

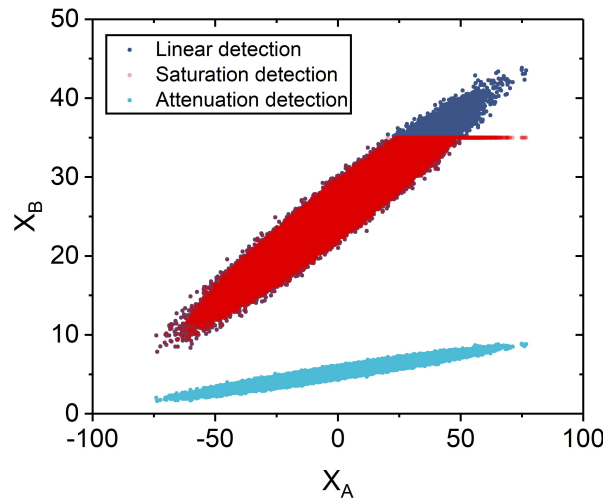


Figure 3. Measurement results. Red dots: results under the saturation attack; Blue dots: results under saturation attack; Light blue dots: results after being attenuated. Experimental parameters: $X_{\text{sat}}^{\text{Bsat}} = 35\sqrt{N_0}$, $\Delta x = 110$, and $N = 10^7$.

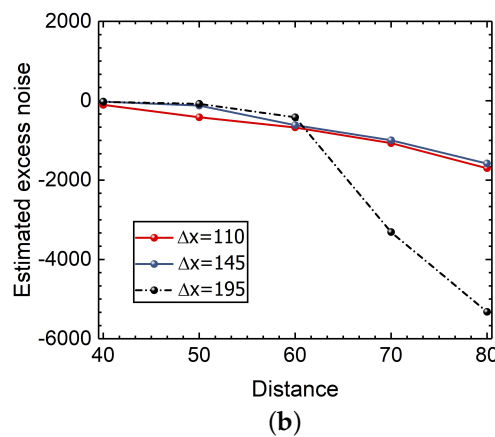
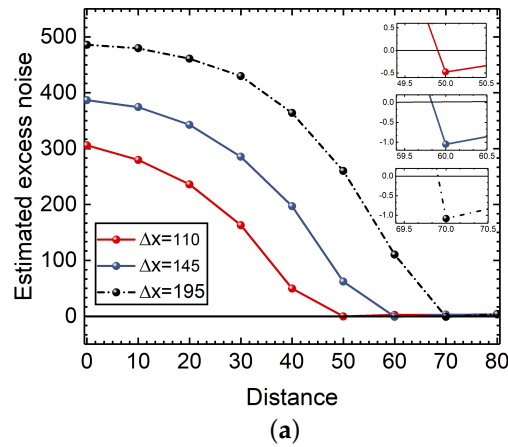


Figure 4. The estimated excess noise of the CVQKD system. (a) The traditional system under saturation attack. (b) The AOF-embedded system under saturation attack.

3.2. Effects on the Secret Key Rate

The secret key rate using reverse reconciliation for the AOF-embedded CVQKD can be expressed as [28,29]

$$K = \beta I_{AB} - \chi_{BE}, \tag{2}$$

where β denotes the reconciliation efficiency, I_{AB} is the mutual information between Alice and Bob, and χ_{BE} is the Holevo bound of Eve's knowledge.

In Appendix C, we demonstrate the effects of parameters gain g and displacement Δx on the performance of the CVQKD system. Without loss of generality, we consider displacement Δx in numerical simulations. As shown in Figure 5a, Alice and Bob can extract the positive secret key rate when the transmission distance is more than 45 km. The large displacement Δx usually results in the long transmission distance. As Alice and Bob can achieve the positive secret key rate, Eve may succeed in stealing information without being discovered, leading to a security loophole. The reason is that when Eve performs the saturation attack, the secret key rate is positive, whereas the estimated excess noise is negative. However, after performing the AOF-enabled counteraction compensation, the secret key rate becomes negative, as shown in Figure 5b. As a consequence, Alice and Bob are able to detect the potential eavesdropper since there is no secret key generated from the resulting system.

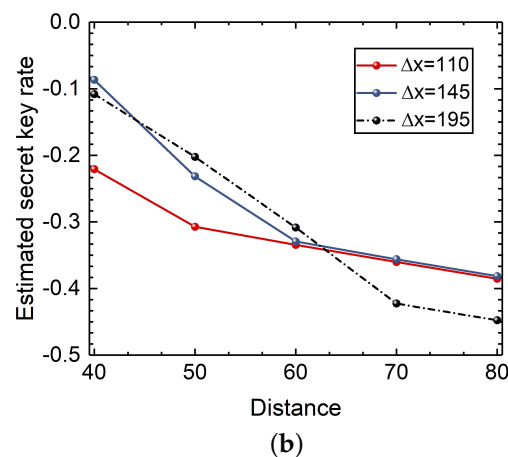
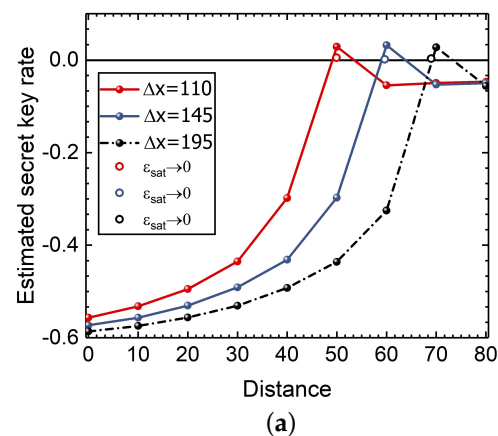


Figure 5. The secret key rate of the CVQKD system. (a) The secret key rate of the traditional system under saturation attack. The hollow dots represent the value evaluated by the excess noise approaching to zero. (b) The secret key rate of the AOF-embedded system.

4. Conclusions

We have proposed an AOF-embedded CVQKD to resist the saturation attack for performance improvement of the practical security. The numerical simulations show that after performing the AOF in the linear domain, the estimated excess noise is made more than zero, and the secret key rate is less than zero. The legal participants can detect Eve, who performs the saturation attack. Based on the AOF-enabled countermeasure compensation, the saturation attack can be broken to enhance the practical security, which provides a useful approach to increasing the practical security of the CVQKD system. In

addition, there might exist other approaches for counteracting a saturation attack, such as the self-adapting detection of the eavesdroppers with machine learning or deep learning, which will be investigated in our future work.

Author Contributions: Conceptualization, S.X.; writing—original draft preparation, Y.L.; writing—review and editing, Y.M.; writing—editing; Y.G. All authors have read and agree to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (Grant Nos. 61871407, 61801522).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Description of the AOF-Based CVQKD Protocol

The AOF-based DM CVQKD protocol is described in the following steps.

- (1) Alice prepares the bipartite state with variance $V = 1 + V_A$ and sends randomly one of the four coherent states to Bob;
- (2) Bob measures randomly X and P by using homodyne detection. Subsequently, the outcomes x_B and p_B are obtained;
- (3) The outcomes produced by the first block are used to calculate the value of attenuation in post-processing with x_A prepared by Alice. The information of the first block can be rejected. The attenuation coefficient is retained and sent to the AOF. Assuming the initial value of attenuation and offset is one. The attenuation coefficient calculated is simultaneously used to update the value of attenuation and offset;
- (4) According to the attenuation updated, AOF performs to attenuate the data before Bob measured. When there is no attenuation coefficient updated, the data can perform the step of offset;
- (5) The excess noise and the key rate are estimated. According to them, Alice and Bob can judge whether the information is safe.

We note that homodyne detection or heterodyne detection can be usually performed in CVQKD. The principle of homodyne detection is to calculate the difference photocurrent by coherently amplifying the reference signal (local oscillator) and modulated signal. The first step of homodyne detection is to calculate the photocurrent \hat{i} . \hat{i} can be obtained by a photodetector that converts the photons into electrons and hence into an electric current. We assume $\hat{i} \propto \hat{n} = \hat{a}^\dagger \hat{a}$ or $\hat{i} = q \hat{a}^\dagger \hat{a}$ where q is a constant. The mode \hat{a} must be combined with a local oscillator by using a 50:50 beam splitter when the mode is detected. We can obtain the photocurrents as follow

$$\hat{i}_1 = q \hat{a}^{\dagger 1} \hat{a}_1 = q(\alpha_{LO}^* + \hat{a}^\dagger)(\alpha_{LO} + \hat{a})/2, \quad (A1)$$

$$\hat{i}_2 = q \hat{a}^{\dagger 2} \hat{a}_2 = q(\alpha_{LO}^* - \hat{a}^\dagger)(\alpha_{LO} - \hat{a})/2. \quad (A2)$$

The difference photocurrent is expressed as

$$\delta \hat{i} = \hat{i}_1 - \hat{i}_2 = q(\alpha_{LO}^* \hat{a} + \alpha_{LO} \hat{a}^\dagger), \quad (A3)$$

which can be used to detect any quadrature by adjusting the phase of local oscillator.

The approach that simultaneously measures the two orthogonal values by using two homodyne detections is heterodyne detection. The amplitude modulation, the frequency modulation, and the phase modulation are used in CVQKD because the local oscillator frequency is not equal to the frequency of signal.

Comparing homodyne detection with heterodyne detection, the squeezed state, and the coherent state as signal sources are more suitable for homodyne detection, and heterodyne detection, respectively. Although heterodyne is better in the coherent state, it produces extra noise. Considering the free-space scenes, it can actively inhibit the interference noise of the atmosphere and obviously filter the noise of the channel by using homodyne detection.

Appendix B. Description of Saturation Attack

Without loss of generality, we assume that Eve’s station is located at Alice’s output and thus the channel transmissions between Alice and Bob, and the channel transmissions between Eve and Bob are equal. The quadratures modulated by Eve can be expressed as

$$X_M = \frac{1}{\sqrt{2}}(X_A + X_0 + X'_0 + X_{N_{A,E}}), \tag{A4}$$

$$X_E = gX_M + \Delta x + X''_0, \tag{A5}$$

where X_M is the results of measurement with the help of heterodyne detection and X_E is the coherent state prepared by Eve on the basis of X_M . Here X_A is a Gaussian random variable with variance V , X_0 denotes a noise-term because of the coherent-state encoding of Alice, X'_0 is a noise-term due to the loss from the heterodyne detection by Eve, and $X_{N_{A,E}}$ is a technical noise of Alice’s preparation and Eve’s measurement process with its variance $\zeta_{A,E}$. In addition, g is considered by Eve to compensate for the loss of the heterodyne detection, Δx represents the displacement chosen by Eve, and X''_0 is a noise term due to the coherent-state encoding of Eve. We note X_0 , X'_0 , and X''_0 follow the variance of $\mathcal{N}(0, N_0)$, where N_0 is the shot noise.

In order to estimate the parameters from Alice’s and Bob’s correlated variables, we consider that the linear detection range is infinite in homodyne detection. The measured quadrature X_{Blin} can be given by

$$X_{Blin} = t(X_E + X_{N_{E,B}}) + \sqrt{1 - t^2}X'''_0 + X_{ele}. \tag{A6}$$

It is a normal linear model parametrized by $t = \sqrt{\eta T}$, where T represents the channel transmission under weak turbulence and the optical transmission including the homodyne detection’s finite efficiency can be signified by η through Bob’s setup. X_{ele} denotes the electronic noise of Bob with $\text{Var}(X_{ele}) = v_{ele}$. Here $X_{N_{E,B}}$ [$\text{Var}(X_{N_{E,B}}) = \zeta_{E,B}$] denotes the technical noise between Eve and Bob, $\sqrt{1 - t^2}X'''_0$ [$\text{Var}(X'''_0) = N_0$] is vacuum noise. All the estimated parameters can be normalized in shot-noise units.

Unfortunately, in practice, the range of the linearity of the homodyne detection cannot be arbitrarily large. A real model should take saturation into account. Eve can employ the saturated detection to attack the system of CVQKD by freely setting the displacement value Δx . The parameter estimation is affected by saturation. Consequently, Eve can fully compromise the practical security of the CVQKD protocol by manipulating the excess noise and the channel transmission estimated by Alice and Bob.

Appendix C. Parameter Estimations

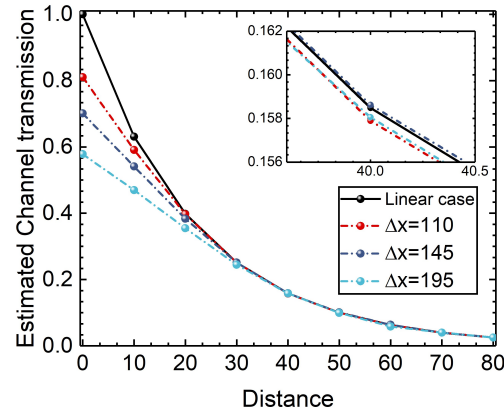
According to the linear model [2], the channel transmission T_{lin} , the variance of Bob $\text{Var}(X_{Blin})$, and correlation of Alice and Bob $\text{Cov}(X_A, X_{Blin})$ can be given by

$$T_{lin} = \frac{\text{Cov}(X_A, X_{Blin})^2}{\eta \text{Var}(X_A)^2}, \tag{A7}$$

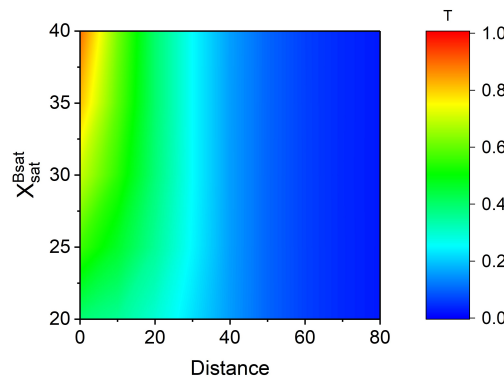
$$\text{Var}(X_{Blin}) = \eta T \frac{G}{2} \text{Var}(X_A) + \frac{G}{2} \eta T \zeta + N_0, \tag{A8}$$

$$\text{Cov}(X_A, X_{\text{Blin}}) = \langle X_A X_{\text{Blin}} \rangle = \frac{tg}{\sqrt{2}} \text{Var}(X_A), \tag{A9}$$

where $\xi = 2N_0 + \xi_{\text{sys}}$, $G = g^2 = \sqrt{2}$ and $\xi_{\text{sys}} = \xi_{A,E} + \frac{2}{G}\xi_{E,B}$. All variances and parameters can be expressed in short noise units.



(a)



(b)

Figure A1. (a) The estimated channel transmission for $X_{\text{sat}}^{\text{Bsat}} = 35\sqrt{N_0}$. (b) The saturation data $X_{\text{sat}}^{\text{Bsat}}$ for $\Delta x = 110$. Experimental parameters: $T = 10^{-aL}$, $a = 0.2$ dB/km, $\eta = 0.55$, $V_A = 16$, $v_{\text{ele}} = 0.015N_0$, and $N = 10^7$.

In practice, the homodyne detection has a finite linearity domain due to the electric characteristics of the homodyne detector, such as the linearity domain of the amplifier or the range of data acquisition (DA) card. The relationship of the measured quadrature X_{Blin} (infinite linearity domain) and the measured quadrature X_{Bsat} in linear range $[-r, r]$ can be expressed as

$$\begin{cases} X_{\text{Blin}} \geq r, & X_{\text{Bsat}} = r; \\ X_{\text{Blin}} = \pm r, & X_{\text{Bsat}} = X_{\text{Blin}}; \\ X_{\text{Blin}} \leq -r, & X_{\text{Bsat}} = -r. \end{cases} \tag{A10}$$

As a consequence, we can deduce the relationship of $\text{Var}(X_{\text{Blin}})$ and $\text{Var}(X_{\text{Bsat}})$. The channel transmission T_{sat} and the excess noise ξ_{sat} can be derived as

$$T_{\text{sat}} = T \frac{G}{8} \left[1 + \text{erf}\left(\frac{r - \Delta}{\sqrt{2\text{Var}(X_{\text{Blin}})}}\right) \right]^2, \tag{A11}$$

$$\begin{aligned} \xi_{\text{sat}} = \frac{1}{\eta T \frac{G}{2} (1+A)^2} & \left[2\text{Var}(X_{\text{Blin}}) \left(1 + A - \frac{B^2}{\pi} \right) - 2\sqrt{\frac{2\text{Var}(X_{\text{Blin}})}{\pi}} \right. \\ & \left. \cdot (r - \Delta)A * B + (r - \Delta)^2 (1 - A^2) - 4N_0 \right] - V_A, \end{aligned} \tag{A12}$$

where the parameter Δ is considered as displacement $\Delta = t\Delta x$, and

$$A = \operatorname{erf}\left(\frac{r - \Delta}{\sqrt{2\operatorname{Var}(X_{\text{Blin}})}}\right), \quad B = \exp\left(-\frac{(r - \Delta)^2}{2\operatorname{Var}(X_{\text{Blin}})}\right). \quad (\text{A13})$$

In Figure A1a, we show the behaviors of T_{sat} versus the transmission distance. As Alice and Bob monitor the channel transmission, they may detect Eve for $T_{\text{sat}} < T$. Therefore, we can design a countermeasure method by regulating the gain g to make $T_{\text{sat}} = T$ satisfying the constraint

$$\frac{2\sqrt{2}}{g} - 1 = \operatorname{erf}\left(\frac{r - \Delta}{\sqrt{\operatorname{Var}(X_{\text{Blin}})}}\right). \quad (\text{A14})$$

In Figure A1b, we show the characteristics of the channel transmission T under the saturation attack, which approaches the linear case as the detector linearity limit $X_{\text{sat}}^{\text{Bsat}}$ increases.

References

1. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2019**, *81*, 1301–1350. [[CrossRef](#)]
2. Qin, H.; Kumar, R.; Alléaume, R. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Phys. Rev. A* **2016**, *94*, 012325. [[CrossRef](#)]
3. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *arXiv* **2020**, arXiv:2003.06557.
4. Ye, W.; Zhong, H.; Liao, Q.; Huang, D.; Hu, L.; Guo, Y. Improvement of self-referenced continuous-variable quantum key distribution with quantum photon catalysis. *Opt. Express* **2019**, *27*, 17186–17198. [[CrossRef](#)]
5. Zhong, H.; Zou, S.; Huang, D.; Guo, Y. Continuous-variable quantum key distribution coexisting with classical signals on few-mode fiber. *Opt. Express* **2021**, *29*, 14486–14504. [[CrossRef](#)]
6. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [[CrossRef](#)]
7. Liao, Q.; Xiao, G.; Xu, C.G.; Xu, Y.; Guo, Y. Discretely modulated continuous-variable quantum key distribution with an untrusted entanglement source. *Phys. Rev. A* **2020**, *102*, 032604. [[CrossRef](#)]
8. Qin, H.; Kumar, R.; Makarov, V.; Alléaume, R. Homodyne-detector-blinding attack in continuous-variable quantum key distribution. *Phys. Rev. A* **2018**, *98*, 012312. [[CrossRef](#)]
9. Braunstein, S.L.; Van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **2005**, *77*, 513. [[CrossRef](#)]
10. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2012**, *84*, 621. [[CrossRef](#)]
11. Huang, P.; Fang, J.; Zeng, G. State-discrimination attack on discretely modulated continuous-variable quantum key distribution. *Phys. Rev. A* **2014**, *89*, 042330. [[CrossRef](#)]
12. Guo, Y.; Ye, W.; Zhong, H.; Liao, Q. Continuous-variable quantum key distribution with non-Gaussian quantum catalysis. *Phys. Rev. A* **2019**, *99*, 032327. [[CrossRef](#)]
13. Zhou, J.; Huang, D.; Guo, Y. Long-distance continuous-variable quantum key distribution using separable Gaussian states. *Phys. Rev. A* **2018**, *98*, 042303. [[CrossRef](#)]
14. Grosshans, F.; Van Assche, G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241. [[CrossRef](#)] [[PubMed](#)]
15. Ye, W.; Zhang, H.; Wei, C.; Zhong, H.; Xia, Y.; Hu, L.; Guo, Y. Nonclassicality and entanglement of single-photon catalysis-assisted two-mode squeezed coherent state. *Opt. Commun.* **2020**, *474*, 126103. [[CrossRef](#)]
16. Liao, Q.; Wang, Y.; Huang, D.; Guo, Y. Dual-phase-modulated plug-and-play measurement-device-independent continuous-variable quantum key distribution. *Opt. Express* **2018**, *26*, 19907–19920. [[CrossRef](#)]
17. Tan, X.; Guo, Y.; Zhang, L.; Huang, J.; Shi, J.; Huang, D. Wavelength attack on atmospheric continuous-variable quantum key distribution. *Phys. Rev. A* **2021**, *103*, 012417. [[CrossRef](#)]
18. Mao, Y.; Huang, W.; Zhong, H.; Wang, Y.; Qin, H.; Guo, Y.; Huang, D. Detecting quantum attacks: A machine learning based defense strategy for practical continuous-variable quantum key distribution. *New J. Phys.* **2020**, *22*, 083073. [[CrossRef](#)]
19. Qi, B.; Huang, L.L.; Qian, L.; Lo, H.K. Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Phys. Rev. A* **2007**, *76*, 052323. [[CrossRef](#)]
20. Jain, N.; Wittmann, C.; Lydersen, L.; Wiechers, C.; Elser, D.; Marquardt, C.; Makarov, V.; Leuchs, G. Device calibration impacts security of quantum key distribution. *Phys. Rev. Lett.* **2011**, *107*, 110501. [[CrossRef](#)]
21. Li, H.W.; Wang, S.; Huang, J.Z.; Chen, W.; Yin, Z.Q.; Li, F.Y.; Zhou, Z.; Liu, D.; Zhang, Y.; Guo, G.C.; et al. Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. *Phys. Rev. A* **2011**, *84*, 062308. [[CrossRef](#)]
22. Guo, Y.; Xie, C.; Liao, Q.; Zhao, W.; Zeng, G.; Huang, D. Entanglement-distillation attack on continuous-variable quantum key distribution in a turbulent atmospheric channel. *Phys. Rev. A* **2017**, *96*, 022320. [[CrossRef](#)]

23. Huang, J.Z.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Li, H.W.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A* **2013**, *87*, 062329. [[CrossRef](#)]
24. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A* **2013**, *87*, 062313. [[CrossRef](#)]
25. Mao, Y.; Wang, Y.; Huang, W.; Qin, H.; Huang, D.; Guo, Y. Hidden-Markov-model-based calibration-attack recognition for continuous-variable quantum key distribution. *Phys. Rev. A* **2020**, *101*, 062320. [[CrossRef](#)]
26. Huang, J.Z.; Kunz-Jacques, S.; Jouguet, P.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum hacking on quantum key distribution using homodyne detection. *Phys. Rev. A* **2014**, *89*, 032304. [[CrossRef](#)]
27. Wu, X.; Wang, Y.; Guo, Y.; Zhong, H.; Huang, D. Passive continuous-variable quantum key distribution using a locally generated local oscillator. *Phys. Rev. A* **2021**, *103*, 032604. [[CrossRef](#)]
28. Liu, W.; Xu, Z.; Jin, X. Saturation compensation for visible light communication with off-the-shelf detectors. *Opt. Express* **2021**, *29*, 9670–9684. [[CrossRef](#)]
29. Huang, D.; Huang, P.; Lin, D.; Wang, C.; Zeng, G. High-speed continuous-variable quantum key distribution without sending a local oscillator. *Opt. Lett.* **2015**, *40*, 3695–3698. [[CrossRef](#)]