Pis'ma v ZhETF, vol. 124, iss. 6, pp. 504 – 506

Unidimensional-modulation continuous-variable quantum key distribution under light-injection attacks

P. Wang[1)], *J. Liang, Z. Bai, L. Chang*

School of Information, Shanxi University of Finance and Economics, 030006 Taiyuan, China

Submitted 10 August 2026
Resubmitted 19 August 2026
Accepted 19 August 2026

Unidimensional-modulation continuous-variable quantum key distribution has received considerable attention due to its simplified transmitter architecture, reduced random-number consumption, and low deployment cost. However, its security against source-side light-injection attacks remains unexplored. In this paper, the effects of such attacks on unidimensional-modulation continuous-variable quantum key distribution systems are systematically investigated. A theoretical model of quantum-state preparation at the transmitter under light-injection attacks is established, parameter estimation bias formulas are derived, the resulting degradation in the secret key rate is quantified, and the theoretical results are validated through numerical simulations. In addition, the security implications of light-injection attacks in the finite-size regime are examined. The results demonstrate that light-injection attacks cause overestimation of the channel transmittance and underestimation of excess noise. Under finite-size conditions, these attacks reduce the minimum data-block length required to achieve a positive secret key rate, thereby creating a false indication of security even when no secure key can actually be generated. These findings demonstrate that light-injection attacks constitute a serious threat to unidimensional-modulation continuous-variable quantum key distribution systems and provide an important theoretical foundation for future secure practical deployment.

DOI: 10.7868/S3034576626090247

Continuous-variable quantum key distribution (CV-QKD) enables information-theoretically secure key exchange over optical fiber networks, serving as a core technology for next-generation quantum-secure communication systems [1–7]. The unidimensional-modulation CV-QKD (UD CV-QKD) protocol, which encodes key information on only one quadrature (either amplitude or phase) via a single optical modulator, has attracted widespread attention for its simplified transmitter structure, lower random-number consumption and reduced deployment cost, making it a highly competitive scheme for practical metropolitan quantum communication [8–20]. However, practical QKD systems face side-channel security risks caused by device imperfections. Light-injection attack, as a typical source-side attack, allows an eavesdropper to inject external classical light into the transmitter to alter the operating characteristics of optical components, thereby distorting the prepared quantum states and inducing biased parameter estimation [21–27]. While the impact of such attacks on conventional two-dimensional CV-QKD has been extensively studied, the security of UD CV-QKD under light-injection attacks remains to be systematically clarified.

In this work, we present a comprehensive security analysis of source-side light-injection attacks against UD CV-QKD systems. We first establish a physical model for quantum state preparation at the transmitter under light injection, and introduce an intensity-scaling factor k to quantify the attack intensity. Through theoretical derivation, we prove that when the legitimate parties are unaware of the attack, the estimated channel transmittance will be overestimated by a factor of k, while the estimated excess noise will be underestimated by a factor of $1/k$. This systematic bias leads the communicating parties to calculate a secret key rate significantly higher than the actual secure value, leaving the attack undetected within the system noise floor.

We further evaluate the secure key rate using the standard entanglement-based approach under reverse reconciliation, and derive the covariance matrix of the system considering channel loss, excess noise and detector imperfections. To ensure unconditional security, we apply the Heisenberg uncertainty principle as a physical constraint on the phase-quadrature correlation term, and obtain the provably secure key rate by minimizing over the eavesdropper's optimized strategy. For practi-

[1)]e-mail: wangpu@sxufe.edu.cn

cal finite-size scenarios [28], we incorporate statistical fluctuations of parameter estimation by using conservative confidence bounds based on standard normal distribution quantiles, and analyze the finite-size secret key rate considering parameter estimation failure probability and privacy amplification correction.

Figure 1 shows the secret key rate as a function of transmission distance under different attack intensities. The curve for $k = 1$ represents the attack-free

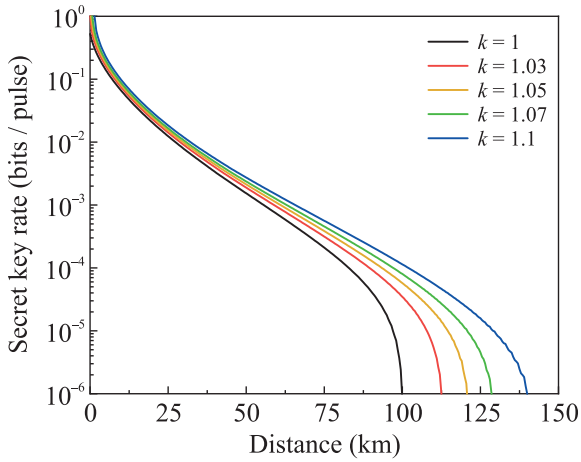

Fig. 1. (Color online) Secret key rate versus transmission distance under different light-injection attack intensities ($k = 1$, 1.03, 1.05, 1.07, 1.1)

benchmark, with a maximum secure transmission distance of approximately 100 km. As the attack intensity k increases, the key rate curves shift upward and extend to longer distances, indicating that the system overestimates both the achievable key rate and the maximum transmission distance. When $k = 1.05$, the maximum transmission distance increases to approximately 120 km, which is 20 km greater than that in the attack-free case. This behavior is consistent with the theoretical analysis, which indicates that light-injection attacks systematically overestimate channel transmittance and underestimate excess noise, thereby producing an overly optimistic evaluation of channel quality. Further simulation results show that the overestimation effect becomes more significant with the increase of channel loss and excess noise. Remarkably, under channel conditions where no positive key rate can be achieved without attack, the attack can still cause the system to incorrectly predict a positive key rate, creating a false sense of security. In the finite-size regime, the attack reduces the minimum number of pulses required to obtain a positive key rate, which means the system may misjudge the communication as secure with fewer data.

These results confirm that light-injection attacks pose a serious and non-negligible security threat to practical UD CV-QKD systems. To mitigate this vulnerability, we propose two practical countermeasures: installing a high-isolation optical isolator at the transmitter output to physically block backward-injected light, and integrating a real-time optical power monitoring module to detect abnormal intensity fluctuations and terminate communication when deviations exceed the security threshold. This work provides an important theoretical basis and practical guidance for the secure deployment of UD CV-QKD systems.

Funding. This work was supported by the Natural Science Foundation of Shanxi Province (Grant # 202303021212168).

Conflict of interest. The authors of this work declare that they have no conflicts of interest.

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography", Rev. Mod. Phys. **74**, 145 (2002).
2. C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information", Rev. Mod. Phys. **84**, 621 (2012).
3. F.-H. Xu, X.-F. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices", Rev. Mod. Phys. **92**, 025002 (2020).
4. S. L. Braunstein and P. van Loock, "Quantum information with continuous variables", Rev. Mod. Phys. **77**, 513 (2005).
5. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography", Adv. Opt. Photon. **12**, 1012 (2020).
6. Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, "Continuous-variable quantum key distribution system: Past, present, and future", Appl. Phys. Rev. **11**, 011318 (2024).
7. P. Wang, Y. Tian, and Y. Li, "Advances in continuous variable measurement-device-independent quantum key distribution", Sci. China Inf. Sci. **68**, 180501 (2025).
8. V. C. Usenko and F. Grosshans, "Unidimensional continuous-variable quantum key distribution", Phys. Rev. A **92**, 062337 (2015).
9. P. Wang, X. Wang, J. Li, and Y. Li, "Finite-size analysis of unidimensional continuous-variable quantum key distribution under realistic conditions", Opt. Express **25**, 27995 (2017).
10. P. Wang, X. Wang, and Y. Li, "Security Analysis of Unidimensional Continuous-Variable Quantum Key Distribution Using Uncertainty Relations", Entropy **20**, 157 (2018).

11. D. Bai, P. Huang, Y. Zhu, H. Ma, T. Xiao, T. Wang, and G. Zeng, "Unidimensional continuous-variable measurement-device-independent quantum key distribution", Quantum Inf. Process. **19**, 53 (2019).
12. L. Huang, Y. Zhang, Z. Chen, and S. Yu, "Unidimensional Continuous-Variable Quantum Key Distribution with Untrusted Detection under Realistic Conditions", Entropy **21**, 1100 (2019).
13. S.-Y. Shen, M.-W. Dai, X.-T. Zheng, Q.-Y. Sun, G.-C. Guo, and Z.-F. Han, "Free-space continuous-variable quantum key distribution of unidimensional Gaussian modulation using polarized coherent states in an urban environment", Phys. Rev. A **100**, 012325 (2019).
14. H. Zhang, X. Ruan, X. Wu, L. Zhang, Y. Guo, and D. Huang, "Plug-and-play unidimensional continuous-variable quantum key distribution", Quantum Inf. Process. **18**, 128 (2019).
15. W. Zhao, R. Shi, Y. Feng, and D. Huang, "Unidimensional continuous-variable quantum key distribution with discrete modulation", Phys. Lett. A **384**, 126061 (2020).
16. Y. Bian, L. Huang, and Y. Zhang, "Unidimensional Two-Way Continuous-Variable Quantum Key Distribution Using Coherent States", Entropy **23**, 294 (2021).
17. W. Zhao, R. Shi, X. Wu, F. Wang, and X. Ruan, "Quantum digital signature with unidimensional continuous-variable against the measurement angular error", Opt. Express **31**, 17003 (2023).
18. Y. Li and T. Wang, "Security analysis of unidimensional continuous-variable quantum key distribution with discretized amplitude modulation", J. Phys. B: At. Mol. Opt. Phys. **57**, 145502 (2024).
19. R. Zhao, J. Zhou, R. Shi, and J. Shi, "Unidimensional Continuous Variable Quantum Key Distribution under Fast Fading Channel", Ann. Phys. **536**, 2300401 (2024).
20. P. Wang, J. Liu, Z. Bai, L. Chang, and Y. Tian, "Implementation and Realistic Security of Unidimensional Modulation Continuous-Variable Quantum Key Distribution in Downstream Access Networks", Photonics **12**, 892 (2025).
21. 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).
22. Y. Zheng, P. Huang, A.-Q. Huang, J.-Y. Peng, and G.-H. Zeng, "Practical security of continuous-variable quantum key distribution with reduced optical attenuation", Phys. Rev. A **100**, 012313 (2019).
23. L. Han, Y. Li, H. Tan, W. Zhang, W. Cai, J. Yin, J. Ren, F. Xu, S. Liao, and C. Peng, "Effect of light injection on the security of practical quantum key distribution", Phys. Rev. Appl. **20**, 044013 (2023).
24. Y. Wang, Y. Zheng, C. Fang, H. Shi, and W. Pan, "Light-injection attack against practical continuous-variable measurement-device-independent quantum key distribution systems", Opt. Express **32**, 33656 (2024).
25. Y. Zheng, J. Wu, C. Fang, Y. Wang, W. Pan, and H. Shi, "Security analysis of continuous-variable quantum key distribution systems based on passive state preparation under light-injection attacks", Opt. Commun. **592**, 132266 (2025).
26. Z. Zhou, P. Huang, T. Wang, and G. Zeng, "Security loophole induced by photorefractive effect in continuous-variable quantum key distribution system", Opt. Express **33**, 21736 (2025).
27. Y. Wang, Y. Zheng, C. Fang, H. Shi, and W. Pan, "Quantum Hacking: Induced-Photorefraction Attack on a Practical Continuous-Variable Quantum Key Distribution System", Adv. Quantum Technol. **8**, e2500053 (2025).
28. A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution", Phys. Rev. A **81**, 062343 (2010).