Intensity correlations in decoy-state BB84 QKD systems

Daniil Trefilov,[1,2,3,4,5,*] Xoel Sixto,[1,2,3] Víctor Zapatero,[1,2,3]
Anqi Huang,[6] Marcos Curty,[1,2,3] and Vadim Makarov[4,1,7]

[1] *Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain*
[2] *School of Telecommunication Engineering, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain*
[3] *atlanTTic Research Center, University of Vigo, Vigo E-36310, Spain*
[4] *Russian Quantum Center, Skolkovo, Moscow 121205, Russia*
[5] *National Research University Higher School of Economics, Moscow 101000, Russia*
[6] *Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer Science and Technology, National University of Defense Technology, Changsha 410073, People's Republic of China*
[7] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*

(Dated: June 11, 2024)

The decoy-state method is a prominent approach to enhance the performance of quantum key distribution (QKD) systems that operate with weak coherent laser sources. Current experimental decoy-state QKD setups increase their secret key rate by raising the repetition rate of the transmitter, which can lead to correlations between subsequently emitted optical pulses. This phenomenon leaks information about the encoding settings, including the intensities of the generated signals, thus invalidating a basic premise of decoy-state QKD. Here, we experimentally characterize intensity correlations between the nearest-neigbouring optical pulses in two commercial prototypes of decoy-state BB84 QKD systems and show that they significantly reduce the asymptotic key rate. In addition, we study intensity correlations between pulses spaced further apart (higher-order correlations) and find that, in contrast to what has been conjectured, their impact on the intensity of the generated signals can be much higher than that of the nearest-neighbour (first-order) correlations.

Quantum key distribution (QKD) represents a method for achieving information-theoretic security when sharing a secret key between distant parties. Practical implementations of QKD encounter challenges and limitations associated with current technology, which might lead to security loopholes. To address these discrepancies between theory and practice, manufacturers of QKD equipment can apply improved security proofs that can handle device imperfections and/or incorporate advanced hardware solutions.

Nevertheless, there remain specific challenges to address for QKD to attain widespread adoption as a technology. A crucial hurdle involves enhancing the secret key rate produced by existing experimental prototypes. Various experimental demonstrations have been conducted with an increased pulse repetition rate of the sources, with the operating frequencies in the GHz regime [1]. Yet, the presence of memory effects in the optical modulators and their controlling electronics leads to correlations among the generated optical pulses [2], thus invalidating most security proofs. Significantly, if this phenomenon is not adequately considered, it can introduce a security vulnerability in the form of information leakage.

On the experimental side, a few recent works have quantified the strength of pulse correlations for various particular QKD system prototypes [1–4], and showed that such correlations are, in general, not negligible. However, more experimental efforts are needed to accurately characterize pulse correlations of arbitrary order in QKD systems that are already available on the market.

In this work, we observe strong intensity correlations in two different commercial prototypes of decoy-state BB84 QKD systems with polarisation encoding. We experimentally prove that, in some cases, higher-order correlations affect the intensities of pulses equally or even more than their nearest neighbours. Moreover, we quantify the impact of this vulnerability on the performance of the QKD systems in terms of their secret key rate by applying a security proof for the cases of first- and second-order correlations [5, 6].

[1] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Performance and security of 5 GHz repetition rate polarization-based quantum key distribution," Appl. Phys. Lett. **117**, 144003 (2020).

[2] K. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, and A. Tomita, "Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses," npj Quantum Inf. **4**, 8 (2018).

[3] X. Kang, F.-Y. Lu, S. Wang, J.-L. Chen, Z.-H. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, G.-J. Fan-Yuan, G.-C. Guo, and Z.-F. Han, "Patterning-effect calibration algorithm for secure decoy-state quantum key distribution," J. Lightwave Technol. **41**, 75–82 (2023).

[4] F.-Y. Lu, Z.-H. Wang, S. Wang, Z.-Q. Yin, J.-L. Chen, X. Kang, D.-Y. He, W. Chen, G.-J. Fan-Yuan, G.-C. Guo, and Z.-F. Han, "Intensity tomography method for secure and high-performance quantum key distribution," J. Lightwave Technol. **41**, 4895–4900 (2023).

[5] V. Zapatero, Á. Navarrete, K. Tamaki, and M. Curty, "Security of quantum key distribution with intensity correlations," Quantum **5**, 602 (2021).

[6] X. Sixto, V. Zapatero, and M. Curty, "Security of decoy-state quantum key distribution with correlated intensity fluctuations," Phys. Rev. Appl. **18**, 044069 (2022).

* dtrefilov@vqcc.uvigo.es