Intensity correlations in decoy-state BB84 quantum key distribution 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
trefdanil@gmail.com

Introduction

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].

Acknowledgement

The Ministry of Science and Education of Russia (program NTI center for quantum communications), Russian Science Foundation (grant 21-42-00040), the Galician Regional Government (consolidation of research units: atlanTTic), MICIN with funding from the European Union NextGenerationEU (PRTR-C17.I1), the Galician Regional Government with own funding through the "Planes Complementarios de I+D+I con las Comunidades Autónomas" in Quantum Communication, the Spanish Ministry of Economy and Competitiveness (MINECO), Fondo Europeo de Desarrollo Regional (FEDER) through grant PID2020-118178RBC21, the European Union's Horizon Europe Framework Programme under the Marie Skłodowska-Curie grant 101072637 (project QSI) and the project "Quantum Security Networks Partnership"(QSNP, grant 101114043), the National Natural Science Foundation of China (grants 62371459 and 62061136011), and the Innovation Program for Quantum Science and Technology (grant 2021ZD0300704). X.S. acknowledges support from FPI predoctoral scholarship granted by the Spanish Ministry of Science, Innovation and Universities.

Reference

[1] F. Grünenfelder et al., *Appl. Phys. Lett.*, 117, 144003 (2020).
[2] K. Yoshino et al., *npj Quantum Inf.*, 4, 8 (2018).
[3] X. Kang et al., *J. Lightwave Technol.*, 41, 75 (2023).
[4] F.-Y. Lu et al., *J. Lightwave Technol.*, 41, 4895 (2023).
[5] V. Zapatero et al., Quantum, 5, 602 (2021).
[6] X. Sixto et al., *Phys. Rev. Appl.*, 18, 044069 (2022).