Simplified Quantum Key Distribution Implementation Secure against State Preparation Flaws

Ainhoa Agulleiro[1,2,3], Fadri Grünenfelder[1,2,3,4], Raphaël Houlmann[4], Ana Blázquez[1,2,3], Hugo Zbinden[1,2,3], Davide Rusca[1,2,3]

[1]*Vigo Quantum Communication Center, Univerity of Vigo, E-3610, Vigo, Spain*

[2]*Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, E-36310, Vigo Spain*

[3]*AtlanTTic Research Center, University of Vigo, E-36310, Vigo Spain*

[4]*Department of Applied Physics, University of Geneva, 1205, Geneva, Switzerland*

We present a fiber-based implementation of a simplified three-state BB84 protocol [1] that accounts for state preparation flaws (SPFs). Alice uses time-bin encoding to create her states, while Bob measures the time of arrival in the Z basis and checks the interference in the X basis. To do so, he uses a superconducting nanowire single-photon detector per basis. In contrast to previous similar implementations [2,3], we leave enough separation between rounds such that there is no overlap between the side bins in Bob's X measurement. This simplifies the state characterization. Indeed, we are able to measure the SPFs by simply running the protocol and letting Bob reveal all of his bits to Alice. We performed the secret key exchange for different quantum channel lengths and compared the results by using the security analysis of [1] or our adaptation of the loss-tolerant method [4] to our protocol. The former assumes perfect state preparation while the latter makes use of our characterization of the SPFs. Our experimental results show that the invalid assumption of perfect state preparation may lead to an underestimation of the phase error rate. With our results, we prove security for the simplified BB84 protocol already used in the high-key experiment of [2] and over long distance [3] even in the presence of SPFs, and we achieve a secret key rate of 2.75×10^4bps over a QC channel of 151km of ULL fiber.

Funding acknowledgement

We acknowledge support from the Galician Regional Government (consolidation of Research Units: AtlantTIC), MICIN with funding from the European Union NextGenerationEU (PRTR-C17.I1) and the Galician Regional Government with own funding through the "Planes Complementarios de I+D+I con las Comunidades Autónomas" in Quantum Communication, the "Hub Nacional de Excelencia en Comunicaciones Cuánticas" funded by the Spanish Ministry for Digital Transformation and the Public Service and the European Union NextGenerationEU, the European Union's Horizon Europe Framework Programme under the Marie Sklodowska-Curie Grant No. 101072637 (Project QSI) and the project "Quantum Security Networks Partnership" (QSNP, Grant No. 101114043), and the European Union via the European Health and Digital Executive Agency (HADEA) under the Project QuTechSpace (Grant No. 101135225). We also acknowledge support through the grant "Programa de axudas á etapa predoutoral da Xunta de Galicia (Consellería de Educación, Ciencia, Universidades e Formación Profesional)" co-funded by the European Union under the Programa FSE+ Galicia 2021-2027".

References

[1] D. Rusca, A. Boaron, M. Curty, A. Martin, and H. Zbinden, Phys. Rev. A 98(5), 052336 (2018).

[2] F. Grünenfelder, A. Boaron, G.V. Resta *et al*., Nat. Photon. 17, 422–426 (2023).

[3] A. Boaron, G. Boso, D. Rusca *et al.*, Phys. Rev. Lett. 121, 190502 (2018).

[4] K. Tamaki, M. Curty, G. Kato, H. K. Lo and K. Azuma, Phys. Rev. A 90, 052314 (2014).