High-Rate Quantum Key Distribution with Time-Bin Qudits

Daniel J. Gauthier,[1] Nurul T. Islam,[2] Charles Lim,[3] Clinton Cahall,[4] and Jungsang Kim[4]

[1]Department of Physics, The Ohio State University, 191 West Woodruff Ave., Columbus, Ohio 43210 USA

[2]Department of Physics and the Fitzpatrick Institute for Photonics, Duke University, Durham, North Carolina 27708, USA

[3]Department of Electrical and Computer Engineering, National University of Singapore, Singapore

[4]Department of Electrical Engineering and the Fitzpatrick Institute for Photonics, Duke University, Durham, North Carolina 27708, USA

Abstract

Development of quantum-proof cryptographic systems is important for cybersecurity in the forthcoming era of quantum computers. Quantum key distribution (QKD) offers one promising solution [1], although the key rate needs to be increased substantially to approach current digital communication rates. Here, we present a discrete-variable QKD system based on time-bin quantum photonics states that allows us to optimize the system performance and achieve record-setting secret key rates of 26.2, 11.9, 7.71, 3.40 and 1.07 Mbps with channel losses of 4, 8, 10, 14 and 16.6 dB, respectively, corresponding to transmission distances of 20, 40, 50, 70 and 83 km in standard telecommunication optical fiber. Our system (Fig. 1) uses high-dimensional states, allowing us to transmit more secret information per received photon and tolerate high quantum channel noise [2–4], and the use of high-efficiency and low-temporal-jitter single- photon-counting detectors allows us to achieve high rates. Our analysis accounts for generalized (coherent) attacks, the finite length of the exchanged key, and a broad class of experimental imperfections. Notably, our system is constructed using off-the-shelf components, is highly scalable, and well suited for either free-space or fiber-based communication systems.

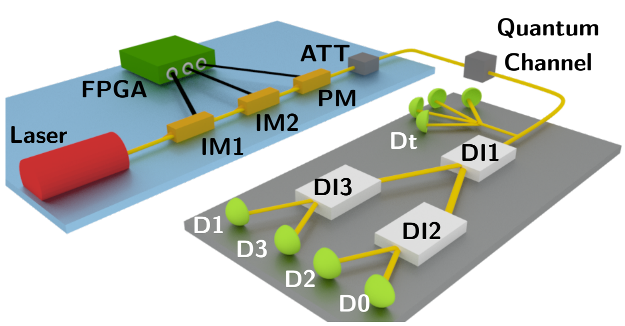

FIG. 1. Alice prepares quantum states in three different intensities by modulating a continuous-wave laser with three intensity modulators (only two are shown for clarity), and a phase modulator. The entire system is time synchronized with a stable clock on a field-programmable gate array (FPGA), which is also used to drive all intensity modulators. The FPGA is programmed to generate time and phase basis states with biased probabilities of 0.90 and 0.10, respectively. An attenuator (ATT) is used to reduce the mean photon numbers to the the single-photon regime. The quantum channel is simulated using a second attenuator whose attenuation is varied to emulate different channel condition. The incoming quantum states in the receiver are split using a 90/10 beamsplitter (BS) to direct 90% of the states for the time-basis measurement and 10% for phase basis measurement. After the initial splitting, the 90% of the states propagating towards the time-basis measurement device is split further into four ways to couple into four detectors.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002).

[2] T. Brougham, S. M. Barnett, K. T. McCusker, P. G. Kwiat, and D. J. Gauthier, Journal of Physics B: Atomic, Molecular and Optical Physics 46, 104010 (2013).

[3] M. Mirhosseini, O. S. Magana-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, New Journal of Physics 17, 033033 (2015).

[4] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits, S. W. Nam, F. Marsili, M. D. Shaw, Z. Zhang, L. Wang, D. Englund, G. W. Wornell, J. H. Shapiro, and F. N. C. Wong, New Journal of Physics 17, 022002 (2015).