[INVITED] Implementation of Quantum Key Distribution with Composable Security Against Coherent Attacks using Einstein-Podolsky-Rosen Entanglement

Roman Schnabel,[1,2,*] Tobias Gehring,[2,3] Vitus Händchen,[2] Jörg Duhme,[4]
Fabian Furrer,[5] Torsten Franz,[4,6] Christoph Pacher,[7] and Reinhard F. Werner[4]

[1]*Institut für Laserphysik und Zentrum für Optische Quantentechnologien,*
Universität Hamburg, Luruper Chaussee 149, 22761 Hamburg, Germany
[2]*Max-Planck-Institut für Gravitationsphysik (Albert-Einstein-Institut) and*
Institut für Gravitationsphysik, Leibniz Universität Hannover, Callinstraße 38, 30167 Hannover, Germany
[3]*Department of Physics, Technical University of Denmark, Fysikvej, 2800 Kgs. Lyngby, Denmark*
[4]*Institut für Theoretische Physik, Leibniz Universität Hannover, Appelstraße 2, 30167 Hannnover, Germany*
[5]*Department of Physics, Graduate School of Science, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, Japan, 113-0033*
[6]*Institut für Fachdidaktik der Naturwissenschaften, Technische Universität Braunschweig, Bienroder Weg 82, 38106 Braunschweig, Germany*
[7]*Digital Safety & Security Department, AIT Austrian Institute of Technology GmbH, 1220 Vienna, Austria*

Quantum key distribution (QKD) enables secure communication over public channels without relying on the hardness of mathematical problems. To ensure absolute security the employed QKD system has to withstand coherent attacks, the security of the key has to be composable, and the security analysis has to account for the finite size of the key. Side-channel attacks on the detectors can also compromise the security and have to be prevented. This contribution presents the first implementation of a QKD system where the above is simultaneously taken into account [1]. In a tabletop experiment we use Einstein-Podolsky-Rosen entangled light at 1550 nm to implement a continuous-variable (CV) QKD system with composable finite-size security of the generated key against coherent attacks. Since our implementation is one-sided measurement device independent, attacks for instance on the local oscillator transmitted through the quantum channel, are covered. Attacks on the source of the quantum states are not covered, however, these side-channel attacks can be suppressed to arbitrarily low probabilities by adding optical isolators. The security of our protocol was proven in Ref. [2].

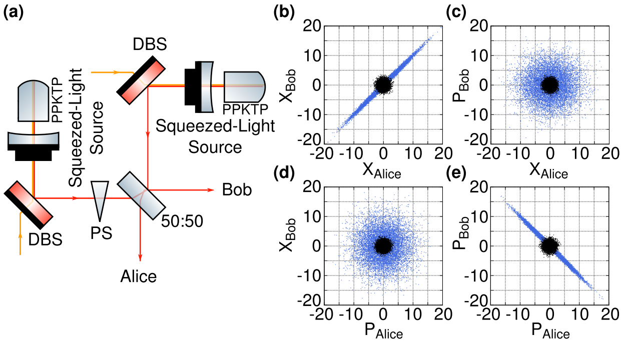

FIG. 1. **Einstein-Podolsky-Rosen entanglement source for CV QKD.** (a) The source consists of two continuous-wave squeezed vacuum beams, generated by type I parametric down-conversion at 1550 nm (red), which are superimposed at a balanced beam splitter with a relative phase of $\frac{\pi}{2}$. Yellow beam: 775 nm pump field, DBS: Dichroic beam splitter, PS: Phase shifter. (b)-(e) Correlations between Alice's and Bob's data, measured by balanced homodyne detection in either the amplitude (X) or phase (P) quadrature. The data is normalized to the noise standard deviation of a vacuum state. Blue: Einstein-Podolsky-Rosen entangled state used for QKD. Black: Reference measurement of zero-point fluctuations of the ground state (vacuum).

Following Ref. [2] our implementation uses measurement variables with continuous spectra [3, 4] and strongly Einstein-Podolsky-Rosen entangled light beams whose actual entanglement strength is a crucial parameter for achieving a positive key rate. The schematic of the experimental setup is illustrated in Fig. 1(a). Two squeezed-light sources, each composed of a nonlinear PPKTP crystal and a coupling mirror, are pumped with a bright pump field at 775 nm (yellow) to produce two squeezed vacuum states at the telecommunication wavelength of 1550 nm (red). The two squeezed vacua, both exhibiting a high squeezing of more than 10 dB, are superimposed at a balanced beam splitter with a relative phase of $\pi/2$, thus generating Einstein-Podolsky-Rosen entanglement. One of the outputs of the beam splitter is kept by Alice, while the other is sent to her communication partner (Bob). Figures 1(b)-(e) show the distribution of measurement outcomes obtained by the two parties measuring either the amplitude (X) or phase (P) quadrature of their respective light field with balanced homodyne detection.

While in our setup Alice and Bob are located on the same optical table, they could in principle be separated and connected by a standard telecommunication fiber. Our implementation is currently limited to a few kilometres due to optical loss in these fibres.

[*] roman.schnabel@physnet.uni-hamburg.de

[1] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, arXiv:1406.6174.
[2] F. Furrer *et al.*, Phys. Rev. Lett. **109**, 100502 (2012).
[3] N. Cerf *et al.*, Phys. Rev. A **63**, 052311 (2001).
[4] C. Weedbrook *et al.*, Rev. Mod. Phys. **84**, 621 (2012).