Experimental Continuous-Variable Oblivious Transfer

Tobias Gehring,[1] Fabian Furrer,[2,3] Christian Schaffner,[4,5]
Christoph Pacher,[6] Roman Schnabel,[7] and Stephanie Wehner[8]

[1] *Department of Physics, Technical University of Denmark, Fysikvej, 2800 Kgs. Lyngby, Denmark*
[2] *NTT Basic Research Laboratories, NTT Corporation,*
3-1 Morinosato-Wakamiya, Atsugi, Kanagawa, 243-0198, Japan.
[3] *Department of Physics, Graduate School of Science,*
University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, Japan, 113-0033.
[4] *Institute for Logic, Language and Computation (ILLC) University of Amsterdam, The Netherlands*
[5] *QuSoft; Centrum Wiskunde & Informatica (CWI); Amsterdam, The Netherlands*
[6] *Center for Digital Safety & Security, AIT Austrian Institute of Technology, 1220 Wien, Austria*
[7] *Institut für Laserphysik und Zentrum für Optische Quantentechnologien,*
Universität Hamburg, Luruper Chaussee 149, 22761 Hamburg, Germany
[8] *QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, Netherlands*

Cryptographic protocols are the backbone of our information society. While quantum key distribution is the most famous two-party protocol which enables secure communication between two trustful parties, all other two-party protocols with protection even against distrustful players can be constructed from the basic primitive called oblivious transfer.

Security of oblivious transfer is established in the noisy-storage model which requires that more quantum signals are sent than a malicious party can reliably store. As scalable and long-lived quantum memories are experimentally still very challenging this assumption can easily be justified.

Here, we present an experimental implementation of oblivious transfer using continuous-variables, see Fig. 1. The implementation is based on entanglement generated by two squeezed light beams interfered at a beam splitter and distributed between two parties. Both parties use homodyne detection with a quadrature angle randomly chosen from two orthogonal ones. Besides the optical implementation a key component of our experiment is a highly efficient non-binary information reconciliation protocol with a success probability larger than 99.9%.

Our work enables the implementation of arbitrary two-party quantum cryptographic protocols with continuous-variable communication systems.

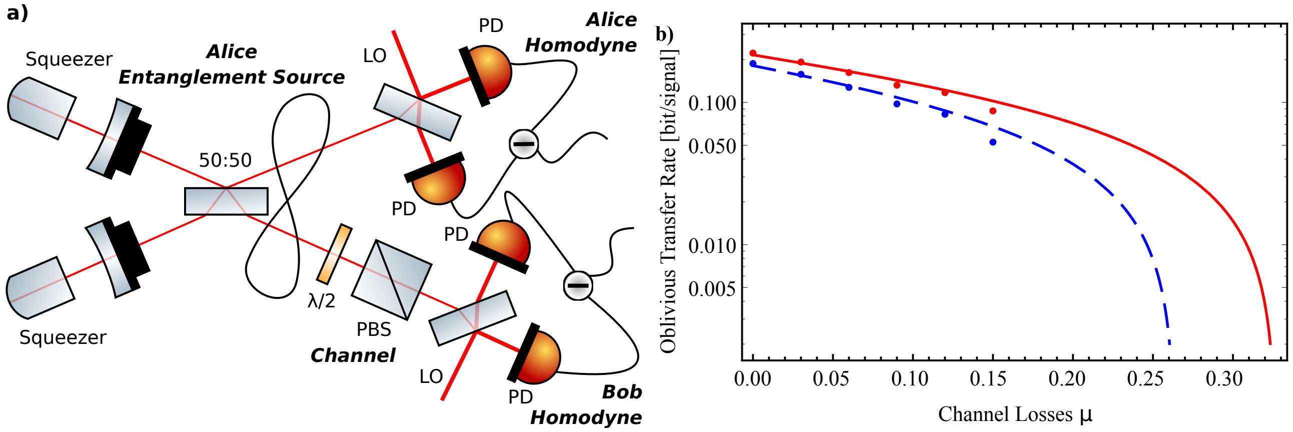

Figure 1: Experimental setup and results. a) Squeezed light at 1550 nm was generated in two parametric down-conversion sources and superimposed at a 50:50 beam splitter to obtain entanglement. One mode was kept locally by Alice and measured with homodyne detection randomly in the amplitude and phase quadrature. The other mode was sent through a free-space channel simulated by a half-waveplate and a polarizing beam splitter (PBS). Bob then performed homodyne detection randomly in amplitude and phase quadrature. PD: Photodiode, LO: Local Oscillator. b) Secure oblivious transfer rate per signal obtained in the experiment. Points correspond to the generated oblivious transfer rates in the experiment for two different storage rates, $\nu = 0.001$ (red) and $\nu = 0.01$ (blue), for quantum memories with a transmittance of 0.75.