

Practical quantum key distribution with polarization entangled photons

A. Fedrizzi, A. Poppe, R. Ursin

Institut für Experimentalphysik, Universität Wien, Boltzmannngasse 5, 1090 Wien, Austria

T. Lorünser, M. Peev, T. Länger

ARC Seibersdorf Research GmbH (ARCS), 2444 Seibersdorf, Austria

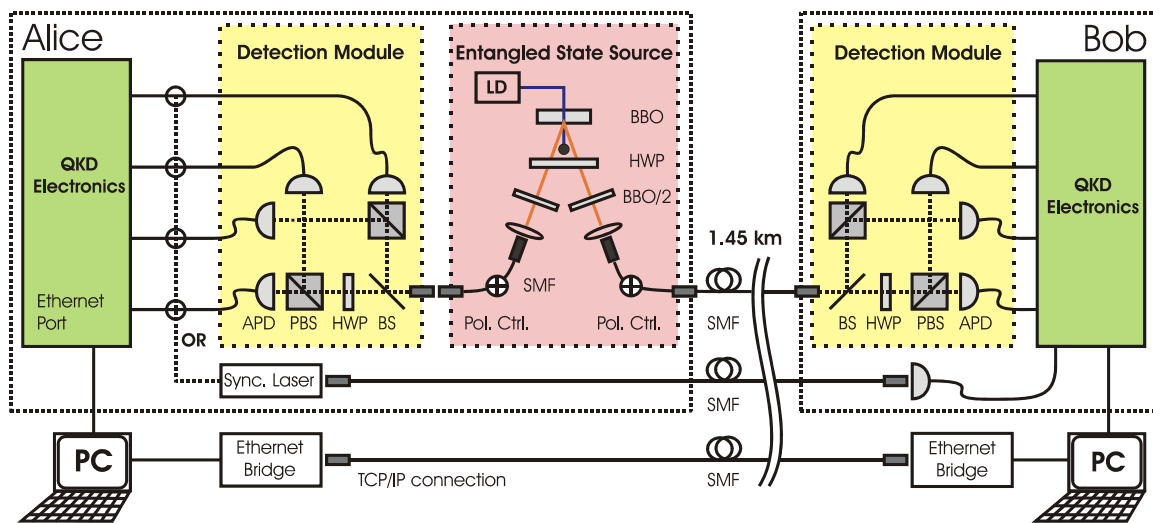
A. Zeilinger

Institut für Experimentalphysik, Universität Wien, Boltzmannngasse 5, 1090 Wien, Austria

Inst. for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmannng. 3, 1090 Wien, Austria

We present an entangled-state quantum cryptography system that operated for the first time in a real-world application scenario in April 2004. It was used for the encryption of an internet bank transfer [1]. This prototype system developed by our group in cooperation with the Austrian Research Centers Seibersdorf (ARCS) was installed at the headquarters of a large bank (Alice) and the Vienna City Hall (Bob). The full key generation protocol was performed in real-time over a fiber bundle of 1.45 km length, installed for this experiment in the Vienna sewage system. The generated quantum key was immediately handed over and used by a secure communication application of order for remittance. Therewith the mayor of Vienna successfully transferred a donation of 3000 Euros to our benefit.

The quantum cryptography system consists of a portable source for polarization-entangled photons, two sets of 4-fold single-photon detection modules with integrated polarization analyzers and embedded hardware devices (QKD Electronics) that handled the complete software protocol needed to extract a secure and private key out of raw detection events. One fiber from the installed bundle was used as the quantum channel. The classical protocol in that experiment was performed via a standard TCP/IP connection. The exposure of the fibers to realistic environmental conditions such as stress and strain during installation, as well as temperature changes were an important feature of this experiment, as the successful operation of the system shows that our system not only works under laboratory conditions.



Sketch of the experimental setup. Our entangled state source produces polarization-entangled photon pairs. One of the photons is locally analyzed in Alice's detection module, while the other is sent over a 1.45 km long single-mode optical fiber (SMF) to the remote site (Bob). When a photon is detected in one of Alice's four APDs, an optical trigger pulse is created (Sync. Laser) and sent over a second fiber to Bob to establish a common time basis.

During the demonstration of the bank wire transfer the data of approx. 3000 bits has to be encoded with a stream of secret bits that was used only once. For the actual transfer a time of slightly more than 30 seconds was used to generate this amount of secret bits performing all steps of the protocol including authentication. That key was generated on demand at the same time as the data for the wire transfer was included in an entry mask. When both were ready, the data were encrypted and sent over a public ethernet connection to the bank. In another mode of operation, continuous generation of a key was also possible, where an application picks secret bits out of the ongoing stream when needed.

[1] A. Poppe et al., Opt. Express **12**, 3865-3871 (2004)