Reliable hands-off entanglement-based QKD system for fiber networks

A. Treiber[1], A. Poppe[3], M. Hentschel[2], T. Lorünser[3], H. Hübel[1], A. Zeilinger[1,2]

[1] Quantum Optics, Quantum Nanophysics and Quantum Information, Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria

[2] Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria

[3]Austrian Research Centers GmbH - ARC, Quantum Technologies Donau-City-Str. 1, 1220 Vienna, Austria

Quantum cryptography or more specifically quantum key distribution (QKD) is the most advanced quantum information protocol. The field has progressed enormously both in theoretical developments and experimental realisations. We present here an entanglement-based QKD system designed to work at 1550nm for optimal distribution in optical fibers[1] using the BBM92[2] protocol. Our QKD system is realised as a compact device. The start-up and alignment is fully automated and stabilisation routines guarantee a hands-off and long-term operation. We show a reliable and stable key generation during a two-week demonstration over a 16km fiber.

Setup

Figure 1a shows an overview of the QKD system, consisting of the units "Alice" and "Bob". The source, located at Alice, produces polarisation entangled photon pairs at highly non-degenerate wavelengths (810nm and 1550nm). The 810nm photons are analysed locally at Alice in four polarisation states (0°, 90°, 45°, 135°) and detected using four Si-APDs. The 1550nm photon is transmitted to Bob using standard single-mode telecom fibers. At Bob, the photons are analysed in the same four polarisations and detected using four InGaAs-APDs. All detection events are processed on FPGA electronics boards. A classical communication channel is used to establish the secret key between Alice and Bob. Trigger pulses (1610nm) are generated at Alice and multiplexed on the quantum channel to gate the InGaAs-APDs at Bob.

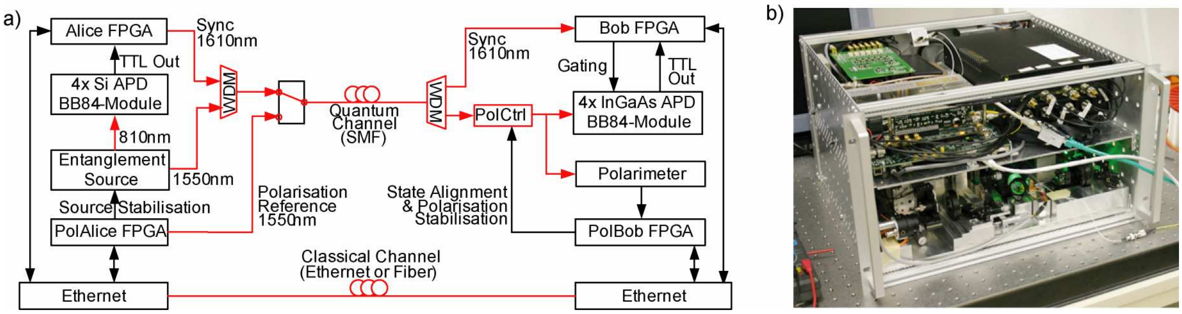

Fig. 1: (a) Scheme of the entanglement based QKD system. (b) The Alice module integrated in a standard 19-inch-box containing the entanglement source at the bottom, the Si-detector array and electronics are found on top. The Bob module is 19-inch compatible as well.

We have implemented several control loops to stabilise the entangled-pair production rate, compensate polarisation drifts in the quantum channel, precisely synchronise the detector gates and align the entangled state ($|\psi^{-}\rangle$) automatically to minimise the error (QBER). All stabilisation modules are controlled by FPGA electronics inside the units of Alice and Bob.

Results

Besides a successful demonstration of a long-term hands-off key generation we could achieve fully automatic start-ups of the complete system even after transportation. The system has been tested intensively during a long-term demonstration over 2 weeks using a deployed standard telecom fiber of 16km length buried underneath the city of Vienna as part of the EU-funded project SECOQC [3]. During this demonstration, a secure bit rate of >2000 bit/s with an average QBER of 3.5% was achieved without any manual intervention. The average entanglement visibility has been 93% with a certainty level of 99.9% to obtain a value higher than 90%.

Conclusion

The QKD device is the first entanglement-based system that can offer long-term operation in an optical fiber network without any user intervention. The results show the maturity reached in two-photon entanglement systems by automatically correcting for environmental changes. The high purity of the shared entangled state makes applications such as QKD possible and hopefully also stimulates the application of other quantum communication protocols in optical fibers.

References

[1] A. Treiber, A. Poppe, M. Hentschel, D. Ferrini, T. Lorünser, E. Querasser, T. Matyus, H. Hübel, and A. Zeilinger, "Fully automated entanglement-based quantum cryptography system for telecom fiber networks", submitted to NJP. arXiv:0901.2725v1

[2] C.H. Bennett, G. Brassard and N.D. Mermin, "Quantum cryptography without Bell's theorem", PRL Vol. 68, no. 5 (1992).

[3] A. Poppe, M. Peev and O. Maurhart, "Outline of the SECOQC quantum-key-distribution network in Vienna", IJQI 6 209 (2008).

978-1-4244-4080-1/09/$25.00 ©2009 IEEE