Quantum Key Distribution with coherent polarization states

Stefan Lorenz, Norbert Lütkenhaus, Jessica Schneider, Oliver Glöckl, Natalia Korolkova, Gerd Leuchs

We present an experimental quantum key distribution with coherent polarization states of light. This is a new concept attempting to combine the strong sides of continuous variable cryptography and single photon cryptography. It possesses the high-bit-rate potential of coherent cryptography using continuous quadrature variables [1], avoids cumbersome local oscillator techniques, is robust against losses due to postselection [2], and provides a possibility to study the transion between continuous variable and single photon regimes, to compare different receiver strategies ranging from homodyning [1] to photon counting [3]. The polarization of the state is described with the quantum Stokes operators S0 (total photon number *n*), S1 (H/V polarization basis), S2 (+-45 deg. polarization basis) and S3 (circular polarization basis). If a state has e.g. a nonvanishing S1, then S2 and S3 are non-commuting observables which can be read out simulteneously only within a quantum uncertainty determined by the mean value of S1.

In the protocol, 4 non-orthorgnal signal states are prepared via fine modulation of polarization around one point on Poincare sphere (S1=*n*, S2=S3=0). The detection at Bob's station is performed in 2 conjugate measurement bases: Bob choose randomly to detect either S2 or S3. For the evaluation of the detected Stokes values the (S2;S3) plane is divided in "+" and "-" half-planes in both measurement directions S2 and S3. The non-orthogonality of the states and non-commutability of S2 and S3 ensures the possibility to create a secret bit sequence. The bit value "1" ("0") is assigned to "+" ("-") measured values. This protocol is a modification of the original coherent quantum cryptography protocol proposed and implemented by the Orsay group [1]. However, in contrast to [1] there is no need for a separate local oscillator beam to be sent with the quantum channel with accurate phase relation, and no mode matching is necessary to interfere the local oscillator with the signal beam. For the Stokes operators, a direct photon number difference measurement play the role of homodyne detection.

The signal state preparation of our protocol is similar to the 4+2 protocol proposed in [3] for weak coherent pulses and single photon detection, whereas the protocol of [1] has its "single photon detection" analogy in BB84 protocol with many bases. A large overlap of the 4 states should be used to ensure security against beam-splitting attacks. The 4 polarization states in our protocol can be described in a two mode picture using a strong reference pulse (S1) and a weak signal pulse (S2,S3), similar to [3]. As the strong reference pulse can be analysed separately, certain manipulations of Eve on the quantum channel can be discerned easily. The formalism of weak signal with strong reference is widely used to analyze optimal detection strategies and security aspects for quantum cryptography with weak coherent pulses and photon counting. It provides therefore a natural apparatus to extend the analysis to the proposed key distribution scheme.

The protocol uses the indistinguishability of overlapping coherent polarization states to generate a secret shared key between two parties. A further essential ingredient is the postselection procedure [2] which allows to overcome the loss limit on the secure transmision range. A polarization measurement cannot distinguish between the 4 overlapping states with

100% accuracy. The reliability of the decision on the signal identity depends on the particular measurement outcome. If the result falls within the region around the bouder between “+” and “-” half-planes, the error probability of this decision is particularly high. We call it “ambiguous result”. For a particular loss level, a boundary should be derived that discriminates between “ambiguous” and “unambiguous” results. This feature is used to create the shared key by postselection [2]. Only those measurements which yield unambiguous results are used for the key generation process, the others are discarded. A potential eavesdropper, who taps off a part of the signal also has ambiguous and unambiguous results, but with a completely independent statistical distribution, due to the quantum nature of the uncertanty. Therefore, discarding less reliable results, Alice and Bob increase their mutual information and decrease that shared with an eavesdropper.

The experimental setup uses a wavelength and temperature stabilized diode laser, which emits cw radiation at 810nm. The beam is modulated in S3 direction by an electro-optical modulator, in S2 direction by a magneto-optical modulator. By using two different S2 and S3 modulations four effective states can be generated.The beam then propagates approx. 30cm distance to Bob's receiver. It consists of passive optical elements to measure the Stokes paramters S2 and S3, and a specifically designed balanced low noise detector. The photocurrent of the detector is recorded on a fast oscilloscope and analysed with special software. The use of only 4 states instead of many Gauss-distributed states of [1] allows for higher raw bit rates not only on the signal preparation side, but also on the receiver side, where one should switch between only two distinct measurements. The measurement basis can be switched in two ways. Either with a second electro-optical modulator, which is driven synchronously with the sender at Alice's site, or by tapping off 50% of the beam to a second detector. One detector is then set to S2 detection, one to S3. This second setup provides an essential increase in raw bit rate and uses the robustness of the postselection scheme against losses (in this case 50% due to the 50:50 beam splitter), so that it is still possible to establish a secret key between sender and receiver for certain modulation types.

We present the preliminary results towards a secrect key generation between sender and receiver. The overlap of the generated states and the resulting error rates on Bob's side have been evaluated. The effects of transmission line losses on the received signal quality were analyzed experimentally. The postselection with different boundaries for the decision on ambigious/unambigious results was performed and the effect of various postselection levels on the achievable raw bit rate and error rate is shown.

[1] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. Cerf, Ph. Grangier, Nature **412**, 238 (2003)
[2] Ch. Silberhorn, T.C. Ralph, N. Lütkenhaus, G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002)
[3] B. Huttner, N. Imoto, N. Gisin, T. Mor, Phys. Rev. A **51**, 1863 (1995)