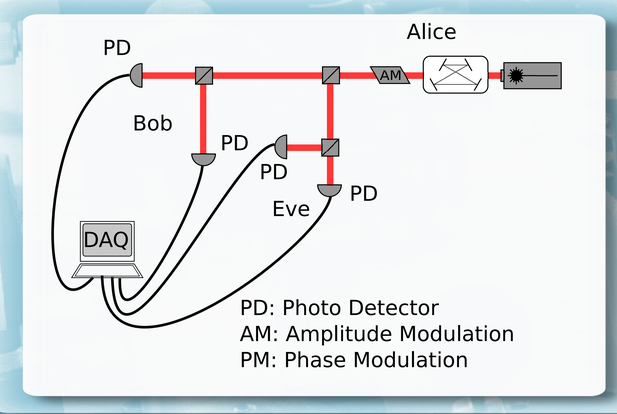
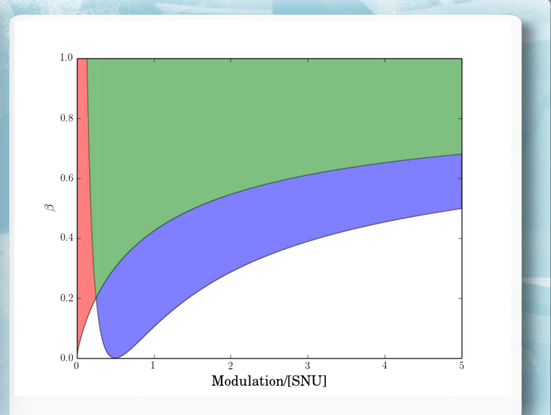
Quantum Key Distribution using Squeezed States of Light

Christian S. Jacobsen[1], Lars S. Madsen[1], Vladyslav Usenko[2], Ulrik L. Andersen[1] and Radim Filip[2]

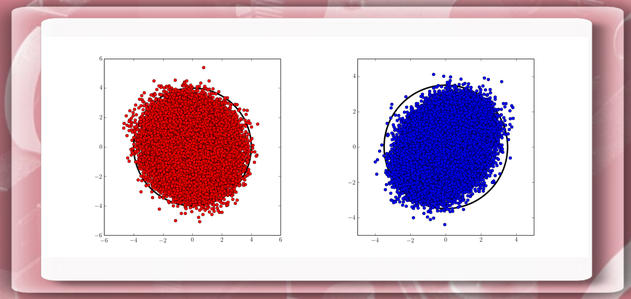
[1]Department of Physics, Technical University of Denmark, Fysikvej, 2800 Kongens Lyngby, Denmark
[2]Department of Optics, Palacký University, 17. listopdau 12, 771 46 Olomouc, Czech Republic

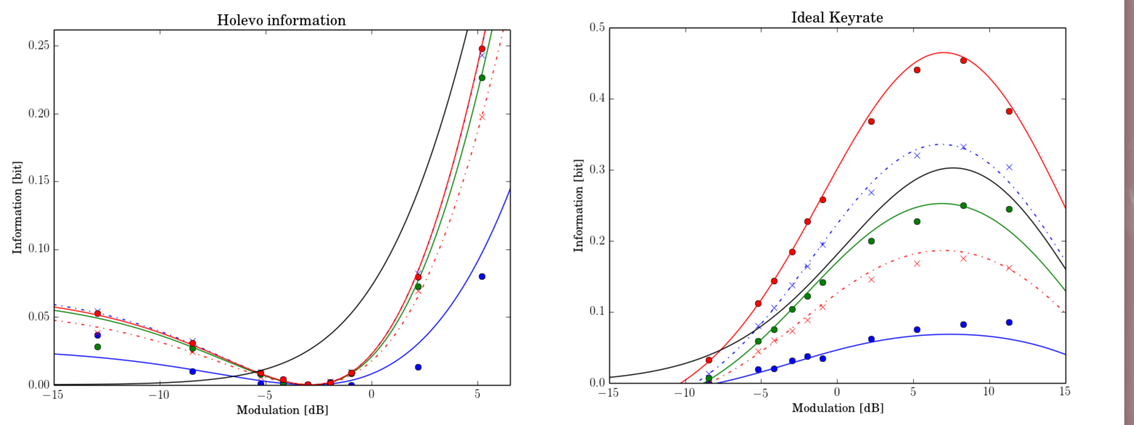
We propose a protocol that completely eliminates Holevo information in the limit of a purely lossy channel. The protocol is based on the observation that the condition $V + V_S = 1$, eliminates the correlations between Bob and Eve in a prepare and measure reverse reconciliation scheme, with V as modulation and V_S as the variance of the state. This condition is realized experimentally by applying a Gaussian distributed modulation of variance V to a squeezed state of variance V_S in the squeezed quadrature.





We experimentally demonstrate the elimination of the Holevo information in the limit of a purely lossy channel. This is visible both in the correlations between the data sets and the calculation of the Holevo information. The maximum in the keyrate is strongly affected by the reconciliation efficiency β and the presence of channel noise, while the location of the minimum in Holevo information is constant for changes in these parameters.



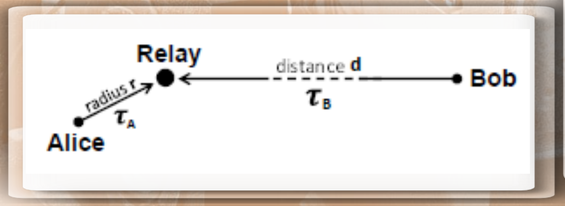


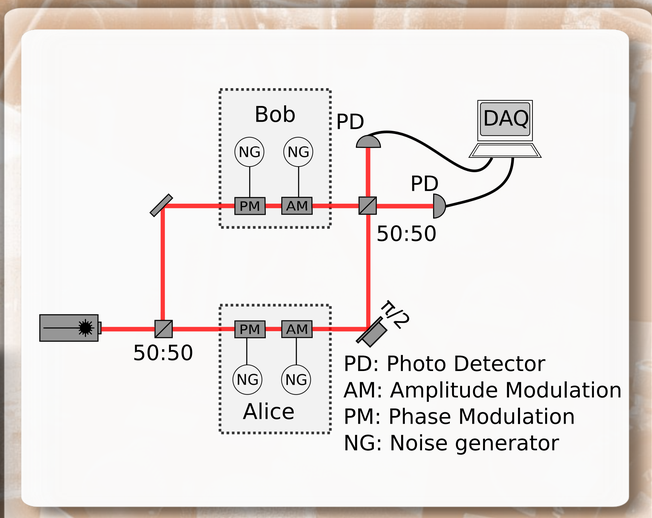
Measuring Device Independent Quantum Key Distribution

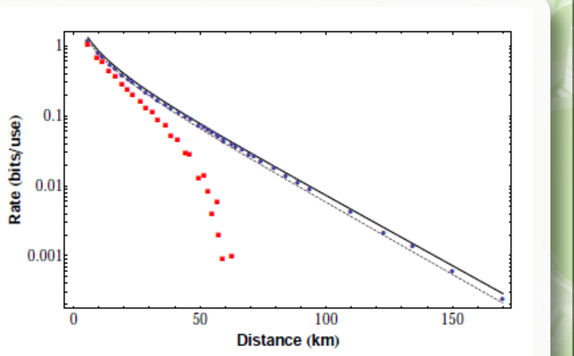
Stefano Pirandola[1], Carlo Ottaviani[1], Gaetana Spedalieri[1], Christian Weedbrook[2], Samuel L. Braunstein[1], Tobias Gehring[3], Christian S. Jacobsen[3] and Ulrik L. Andersen[3]

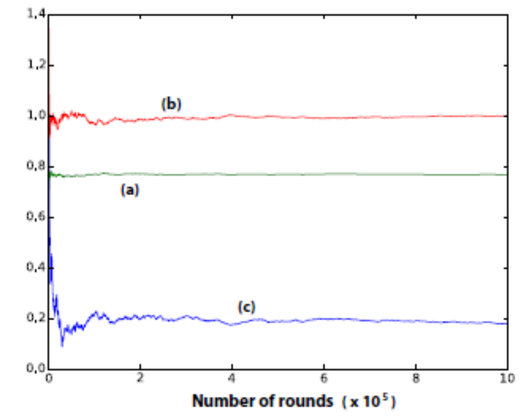
[1]Department of Computer Science, University of York, York YO10 5GH, United Kingdom
[2]Department of Physics, University of Toronto, Toronto, M5S 3G4, Canada
[3]Department of Physics, Technical University of Denmark, Fysikvej, 2800 Kongens Lyngby, Denmark

We propose a protocol where both Alice and Bob produce coherently modulated states in X and P and send them to a relay which is controlled by Eve. At the relay the states are interfered on a beamsplitter and the quadratures X- and P+ are measured and announced to Alice and Bob via a classical channel. Because Alice and Bob know their respective modulations they are able to infer the modulation of the other party and thus establish correlations, while Eve gains no information, because she does not know the individual states. To know the individual states Eve has to launch attacks on the modes before the splitting, introducing transmission loss and even channel noise in the general case. We experimentally demonstrate the robustness of the protocol against these transmission losses in an asymmetric setting where Alice is close to the relay.









For a standard fiber loss of 0.2 dB/km a positive keyrate is obtained from the experimental data, which is well in excess of 100 km, provided that β is unity. The stability of certain important parameters are tested versus data point amount. (a) is the transmissivity estimate, (b) is the collective covariance matrix determinant, which is a symplectic invariant. Finally, (c) is the keyrate. All parameters are seen to stabilize in the limit of many data points, leading to the conclusion that finite size effects are negligible. Below is the theoretical plot predicting that an asymmetric scenario yields higher rates.