

Quantum key distribution robust against photon number splitting attacks.

Steve Brierley
Center for Quantum Information and Communication,
Université Libre de Bruxelles, Belgium

September 7, 2010

Many implementations of quantum key distribution protocols use photons produced by attenuated lasers as a source of quantum states. Such schemes are vulnerable to photon number splitting (PNS) attacks since signals sometimes contain more than one photon. For protocols such as BB84, such attacks greatly reduce the distance over which the protocol remains secure.

In my talk I introduced a new family of quantum key distribution protocols designed to be robust against photon number splitting (PNS) attacks. Each protocol uses d -level quantum states that are elements of c mutually unbiased bases. The case of $d = c = 2$ corresponds to the SARG protocol and we see that by making use of all three mutually unbiased bases ($c = 3$) the protocol is more robust against a PNS attack. When implementing a storage PNS attack the information gained by any eavesdropper is lower than that of the SARG protocol allowing the secure implementation of the protocol over longer distances. Analysis of the protocol against other attacks is given to motivate the claim that the protocol is worthy of further study.

Further details of the protocol can be found in arXiv:0910.2578.