MAR07-2006-020150

Abstract for an Invited Paper
for the MAR07 Meeting of
the American Physical Society

Security of Quantum Key Distribution

NORBERT LÜTKENHAUS, Institute for Quantum Computing, Department of Physics & Astronomy, University of Waterloo

Quantum Key Distribution (QKD) is the most advanced application of Quantum Information Science. It allows extending secret keys over some distances in such a way that the security of the resulting key material can be guaranteed by the laws of quantum mechanics. In contrast to presently used encryption techniques, the security of QKD can be proven in terms of information-theoretic measures. The resulting key can then be used for many tasks, including exchanging secret messages. QKD has been developed in the language of abstract two-level systems, the qubits. They cannot be easily implemented in optical signals. It took some time to bring the protocols and theory of QKD to the point where they fit to the realities of fiber-optical or free-space applications, including lossy channels. Today, QKD schemes can be implemented reliably using standard off-the-shelf components. Information theoretic security is a theoretical concept. Naturally, it is impossible to demonstrate directly that a given experimental set-up indeed creates a secret key. What one can do is to show that the experiment can give data within a certain parameters regime, such as error rate and loss rate, for which a security proof exists. I will discuss what parameter regime gives provable secure key and which parameter regime cannot lead to secret key. It is desirable to prove 'unconditional security,' as it is termed in the world of classical cryptography: no assumption is made about the attacks of an eavesdropper on the quantum channel. However, one has to assume that the signal structure and the measurement device are correctly described by the adopted model and that no eavesdropper can intrude the sender or receiver unit. In this talk I will briefly introduce the concept of QKD and optical implementations. Especially I will discuss security aspects of modern approaches of QKD schemes that allow us to increase the covered distance and the achievable rate.