Quantum Mechanics and Secret Communication

Patrick Zarda, Surasak Chiangga, Thomas Jennewein, Harald Weinfurter
Universität Innsbruck, Institut für Experimentalphysik
Technikerstraße 25, A-6020 Innsbruck, AUSTRIA

One of the fundamental laws of quantum mechanics, the Heisenberg uncertainty relation, tells us that every quantum measurement significantly influences the observed system. Quantum Cryptography utilizes this feature to guarantee secure communication between Alice (transmitter) and Bob (receiver). In wide contrast to the case of classical communication, where an eavesdropper (Eve) would be able to measure the transmitted signals without arresting Alice's or Bob's attention (FIG. 1, left), in Quantum Cryptography eavesdropping can immediately be detected by Alice or Bob (FIG. 1, right).

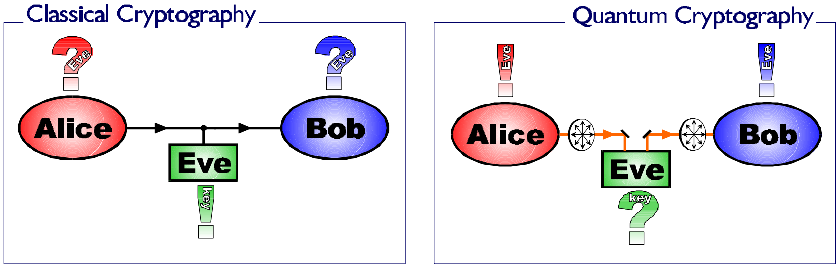

FIG. 1. Eavesdropping in Classical and Quantum Cryptography.

Key-bits can be established by sending polarized photons via a quantum channel (fibre or free space) and detecting them at the other side. Utilizing two polarization directions (H and V) this scheme already can be used to establish a common bit sequence, however it is still unsecure (FIG. 2, left). By using four polarization directions eavesdropping causes errors which can be recognized by Alice and Bob and communication becomes secure (FIG. 2, right) (C.H. Bennett *et al.* 1984).

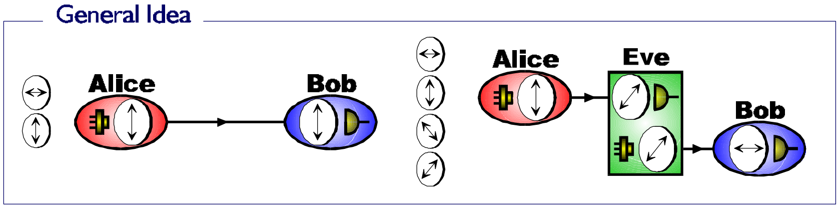

FIG. 2. Secret key distribution by using four polarization directions.

The key distribution requires several steps. Alice sends photons with one of four polarizations, which she has chosen at random. For each photon, Bob chooses at random the type of measurement: either the rectilinear type (H and V) or the diagonal type (+45° and -45°). Bob records the result of his measurement but

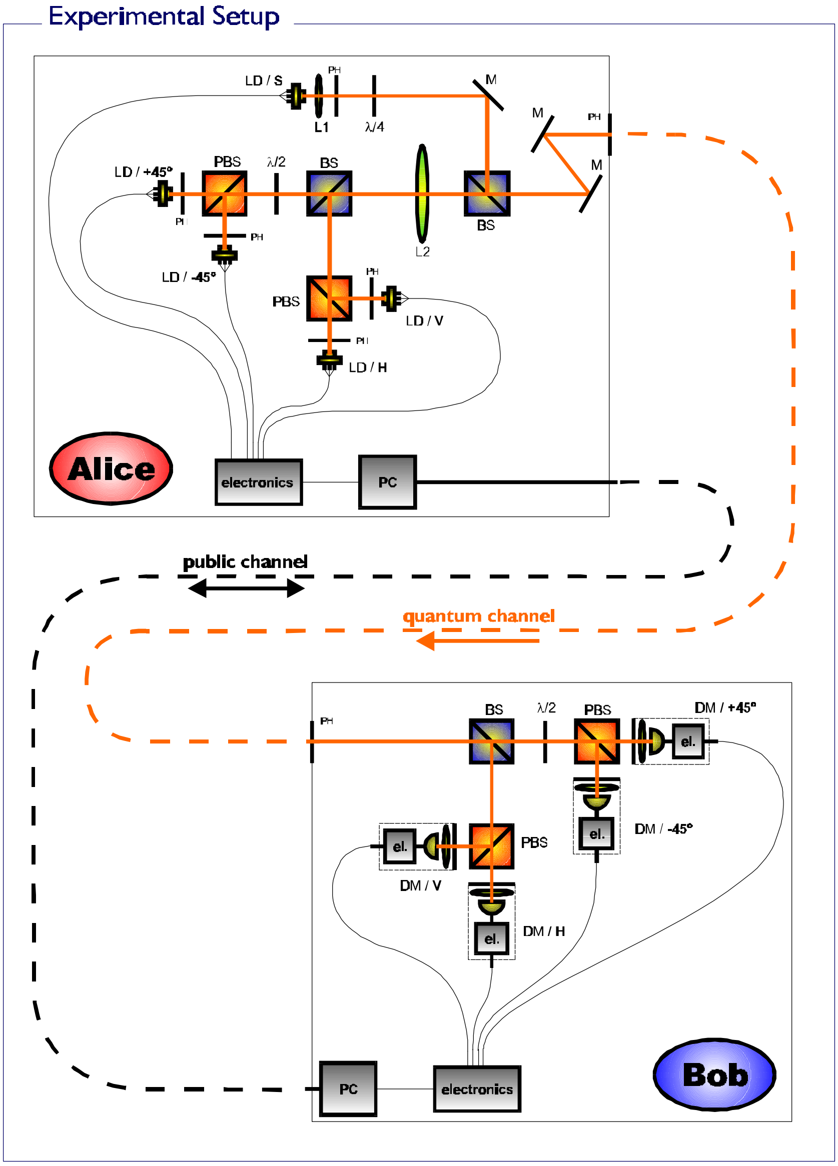

FIG. 3. Setup of our Quantum Cryptography Experiment.

keeps it secret. Bob publicly announces the type of measurement he made, and Alice tells him which measurements were of the correct type. Alice and Bob keep all cases in which Bob measured the correct type. These cases are then translated into bits (1's and 0's) and thereby become the key.
(C.H. Bennett *et al.* 1992, p. 31)

Up to now a couple of Quantum Cryptography experiments were realized. Disadvantages were low bit rates in the Hz-range, large setups on optical tables or complex alignment and management. As a significant difference to other experiments we do not use active components to set or to analyze the four polarization directions. Four laser diodes aligned for the various polarizations (LD/H, LD/V, LD/+45° and LD/-45°) are switched randomly and standard beam splitters are used to combine the different beams (FIG. 3). On Bob's side, we use a 50%/50%-beamsplitter to direct the incoming photon either to an analyzer oriented along H/V or to another one oriented along +45°/-45°. The randomness inherent in quantum mechanics of whether the photon is transmitted or reflected replaces thus any additional, classical random number generator. Synchronization of transmitter and receiver is achieved also over the quantum channel by sending bright circular porarized pulses (LD/S, 20kHz) every 100th weak pulse. The bright pulses cause 4-fold-coincidences on Bob's side where then the original 2MHz-Signal can be reconstructed.

Our measurements show that this compact setup is capable for a fast (pulse rate 2 MHz, effective bit rate kHz-range) and user-friendly Quantum Cryptography key exchange.

Work supported by the Austrian Science Foundation Y-48-PHY.

Correspondence and requests to Patrick Zarda. e-mail: patrick.zarda@uibk.ac.at

C.H. Bennett, and G. Brassard, "An update on quantum cryptography", in: *Advances in Cryptology: Proceedings of Crypto 84,* Springer-Verlag, August 1984, pp. 475 - 480.

C.H. Bennett, G. Brassard, and A.K. Ekert, "Quantum Cryptography", in: *Scientific American*, October 1992, pp. 26-33.