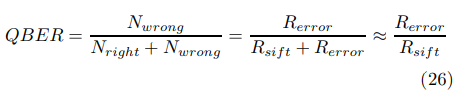
1. **Experimental quantum cryptography with Faint laser pulses**
2. Quantum Bit Error Rate
3. Polarization entanglement
4. Energy-time entanglement
5. Phase-coding
6. Phase-time coding
7. Quantum secret sharing

**A. Quantum Bit Error Rate**

The QBER is defined as the number of wrong bits to the total number of received bits and is normally in the order of a few percent. In the following we will use it expressed as a function of rates:

,

where the sifted key corresponds to the cases in which Alice and Bob made compatible choices of bases, hence its rate is half that of the raw key. The raw rate is essentially the product of the pulse rate frep, the mean number of photon per pulse µ, the probability tlink of a photon to arrive at the analyzer and the probability η of the photon being detected:



The factor q (q≤1, typically 1 or 1 2 ) must be introduced for some phase-coding setups in order to correct for noninterfering path combinations.

One can distinguish three different contributions to Rerror. The first one arises because of photons ending up in the wrong detector, due to unperfect interference or polarization contrast. The rate Ropt is given by the 30In the followin we are considering systems implementing the BB84 protocol. For other protocols some of the formulas have to be slightly adapted. product of the sifted key rate and the probability popt of a photon going in the wrong detector:



This contribution can be considered, for a given set-up, as an intrinsic error rate indicating the suitability to use it for QC. We will discuss it below in the case of each particular system.

The second contribution, Rdet, arises from the detector dark counts (or from remaining environmental stray light in free space setups). This rate is independent of the bit rate. Of course, only dark counts falling in a short time window when a photon is expected give rise to errors.

,

where pdark is the probability of registering a dark count per time-window and per detector, and n is the number of detectors. The two 1 2 -factors are related to the fact that a dark count has a 50% chance to happen with Alice and Bob having chosen incompatible bases (thus eliminated during sifting) and a 50% chance to arise in the correct detector.

Finally error counts can arise from uncorrelated photons, because of imperfect photon sources:

.

This factor appears only in systems based on entangled photons, where the photons belonging to different pairs but arriving in the same time window are not necessarily in the same state. The quantity pacc is the probability to find a second pair within the time window, knowing that a first one was created.

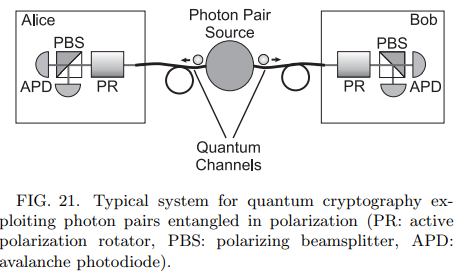
The QBER can now be expressed as follows:

Text, letter

Description automatically generated

**B) Polarization entanglement**

A first class of experiments takes advantage of polarization-entangled photon pairs. The setup, depicted in Fig. 21, is similar to the scheme used for polarization coding based on faint pulses.



A two-photon source emits pairs of entangled photons flying back to back towards Alice and Bob. Each photon is analyzed with a polarizing beamsplitter whose orientation with respect to a common reference system can be changed rapidly. Two experiments, have been reported in the spring of 2000 (Jennewein et al. 2000b, Naik et al. 2000). Both used photon pairs at a wavelength of 700 nm, which were detected with commercial single photon detectors based on Silicon APD’s. To create the photon pairs, both groups took advantage of parametric downconversion in one or two BBO crystals pumped by an argon-ion laser. The analyzers consisted of fast modulators, used to rotate the polarization state of the photons, in front of polarizing beamsplitters.

The group of Anton Zeilinger, then at the University of Innsbruck, demonstrated such a crypto-system, including error correction, over a distance of 360 meters (Jennewein et al. 2000b). Inspir ed by a test of Bell inequalities performed with the same set-up a year earlier (Weihs et al., 1998), the two-photon source was located near the center between the two analyzers. Special optical fibers, designed for guiding only a single mode at 700 nm, were used to transmit the photons to the two analyzers. The results of the remote measurements were recorded locally and the processes of key sifting and of error correction implemented at a later stage, long after the distribution of the qubits. Two different protocols were implemented: one based on Wigner’s inequality (a special form of Bell inequalities), and the other one following BB84.

The group of Paul Kwiat then at Los Alamos National Laboratory, demonstrated the Ekert protocol (Naik et al. 2000). This experiment was a table-top realization with the source and the analyzers only separated by a few meters. The quantum channel consisted of a short free space distance. In addition to performing QC, the researchers simulated different eavesdropping strategies as well. As predicted by the theory, they observed a rise of the QBER with an increase of the information obtained by the eavesdropper. Moreover, they also recently implemented the six-state protocol described in paragraph II D 2, and observed the predicted QBER increase to 33% (Enzer et al. 2001).

The main advantage of polarization entanglement is the fact that analyzers are simple and efficient. It is therefore relatively easy to obtain high contrast. Naik and co-workers, for example, measured a polarization 32 extinction of 97%, mainly limited by electronic imperfections of the fast modulators. This amounts to a QBERopt contribution of only 1.5%. In addition, the constraint on the coherence length of the pump laser is not very stringent (note that if it is shorter than the length of the crystal some difficulties can appear, but we will not mention them here).