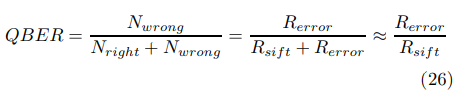
1. **Experimental quantum cryptography with Faint laser pulses**
2. Quantum Bit Error Rate
3. Polarization entanglement
4. Energy-time entanglement
5. Phase-coding
6. Phase-time coding
7. Quantum secret sharing

**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 I 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 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.

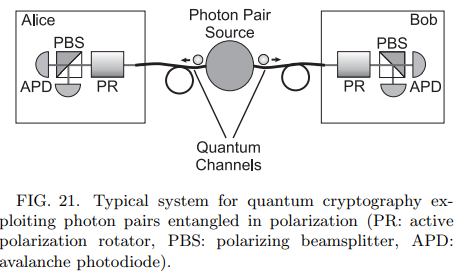
The QBER can now be expressed as follows:

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.



**Experiment:**

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.

**C) Energy-time entanglement**

*1. Phase-coding*

The other class of experiments takes advantage of energy-time entangled photon pairs. The idea originates from an arrangement proposed by Franson in 1989 to test Bell inequalities. As we will see below, it is comparable to the double Mach-Zehnder configuration discussed in section IV C 1. A source emits pairs of energycorrelated photons with both particles created at exactly the same, however uncertain time (see Fig. 22).

This can be achieved by pumping a non-linear crystal with a pump of large coherence time. The pairs of downconverted photons are then split, and one photon is sent to each party down quantum channels. Both Alice and Bob possess a widely, but identically unbalanced MachZehnder interferometer, with photon counting detectors connected to the outputs. Locally, if Alice or Bob change the phase of their interferometer, no effect on the count rates is observed, since the imbalancement prevents any single-photon interference. Looking at the detection-time at Bob’s with respect to the arrival time at Alice’s, three different values are possible for each combination of detectors.

The different possibilities in a time spectrum are shown in Fig. 22. First, both photons can propagate through the short arms of the interferometers. Next, one can take the long arm at Alice’s, while the other one takes the short one at Bob’s. The opposite is also possible. Finally, both photons can propagate through the long arms. When the path differences of the interferometers are matched within a fraction of the coherence length of the down-converted photons, the short-short and the long-long processes are indistinguishable, provided that the coherence length of the pump photon is larger than the path-length difference.

Conditioning detection only on the central time peak, one observes two-photon interferences which depends on the sum of the relative phases in Alice’s and Bob’s interferometer – non-local quantum correlation (Franson 1989) – see Fig. 22. The phase in the interferometers at Alice’s and Bob’s can, for example, be adjusted so that both photons always emerge from the same output port. It is then possible to exchange bits by associating values to the two ports. This is, however, not sufficient. A second measurement basis must be implemented, to ensure security against eavesdropping attempts.

This can be done for example by adding a second interferometer to the systems (see Fig. 23). In the latter case, when reaching an analyzer, a photon chooses randomly to go to one or the other interferometer. The second set of interferometers can be adjusted to also yield perfect correlations between output ports. The relative phase between their arms should however be chosen so that when the photons go to interferometers not associated, the outcomes are completely uncorrelated.

Such a system features a passive state preparation by Alice, yielding security against multiphoton splitting attacks (see section VI J). In addition, it also features a passive basis choice by Bob, which constitutes an elegant solution: neither a random number generator, nor an active modulator are necessary. It is nevertheless clear that QBERdet and QBERacc (defined in eq. (33)) are doubled since the number of activated detectors is twice as high. This disadvantage is however not as important as it first appears since the alternative, a fast modulator, introduces losses close to 3dB, also resulting in an increase of these error contributions. The striking similarity between this scheme and the double Mach-Zehnder arrangement discussed in the context of faint laser pulses in section IV C 1 is obvious when comparing Fig. 24 and Fig. 16! Diagram

Description automatically generatedDiagram

Description automatically generatedDiagram

Description automatically generated Diagram

Description automatically generated

**Study case:**

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). Inspired 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 spite of their qualities, it would be difficult to reproduce these experiments on distances of more than a few kilometers of optical fiber. As mentioned in the introduction to this chapter, polarization is indeed not robust enough to decoherence in optical fibers. In addition, the polarization state transformation induced by an installed fiber frequently fluctuates, making an active alignment system absolutely necessary. Nevertheless, these experiments are very interesting in the context of free space QC.