Distribution of Time-Bin Entangled Qubits over 50 km of Optical Fiber

I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin

Group of Applied Physics-Optique, University of Geneva, CH-1211, Geneva 4, Switzerland

We report experimental distribution of time-bin entangled qubits over 50 km of optical fibers. Using actively stabilized preparation and measurement devices we demonstrate violation of the Clauser-Horne-Shimony-Holt Bell inequality by more than 15 standard deviations without removing the detector noise. In addition we report a proof-of principle experiment of quantum key distribution over 50 km of optical fibers using entangled photon.

In the science of quantum information a central experimental issue is how to distribute entangled states over large distances. Indeed, most protocols in quantum communication require the different parties to share entanglement. The best-known examples are quantum teleportation [1] and Ekert's quantum key distribution (QKD) protocol [2]. Note that even in protocols that do not explicitly require entanglement, like the BB84 QKD protocol [3], security proofs are often based on "virtual entanglement," i.e., on the fact that an ideal single photon source is indistinguishable from an entangled photon pair source in which one photon is used as a trigger [4]. From a more practical point of view, entanglement over significant distances can be used to increase the maximal distance a quantum state can cover, as in quantum repeater [5] and quantum relay [6] protocols. Finally, entanglement is also treated as a resource in the study of communication complexity [7].

As entanglement cannot be created by shared randomness, local operations and classical communication, it must be somehow distributed. Recently there have been some proposals to use satellites for long distance transmission [8]. Also an experiment through open space has been performed transmitting polarization entangled qubits (over 600 m) [9]. Despite the weather and daylight problems, this is an interesting approach. Another possibility, that we follow in this work, is to use the worldwide implemented optical fiber network. This, however, implies some constraints. One should operate at telecommunication wavelengths (1.3 or 1.55 μm), in order to minimize losses in optical fibers, and the encoding of the qubits must be robust against decoherence in optical fibers. Likely the most adequate way to encode qubits is time-bin encoding [10], a discrete version of energy-time entanglement [11]. The major drawback of this kind of encoding, compared to polarization type, is that the creation and the measurement is more complex: it relies on stable interferometers. In this Letter, we report a way to create and to measure time-bin entangled qubits allowing a distribution over 50 km of optical fibers. The two photons still violate Bell inequalities, proving their usefulness for quantum information applications. As an ex-

ample we implement an entanglement based QKD proof-of-principle experiment over this long distance. QKD's goal is the distribution of a secrete key between two parties, traditionally called Alice and Bob (see [12]). QKD is based on a basic quantum mechanical principle: *measuring a quantum system perturbs it* or equivalently on *Heisenberg's uncertainty principle*; it does thus allows Alice and Bob to detect the presence of a spy, called Eve. There are two basic kinds of protocols. In the first one, Alice sends qubits to Bob (BB84-like protocols [3]). In the second one, Alice and Bob each receive half of an entangled state (Ekert-like protocols [2]). In this Letter, we use this second kind of protocols. An advantage that we exploit here is that Alice and Bob can both use passive choices of their measurement bases, thus avoiding the need for fast quantum random number generators.

Let us first remind the reader how to create and measure time-bin entangled qubits. They are created by sending a short laser pulse first through an unbalanced interferometer (denoted as the pump interferometer) and
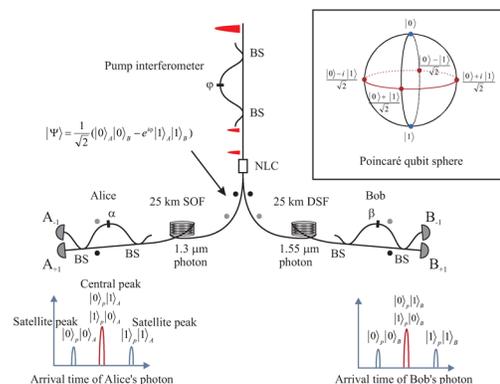

FIG. 1 (color online). Scheme of the experimental setup. Time-bin qubits are prepared by passing a fs pulse through the pump-interferometer and a nonlinear crystal. Eventually, a pair of entangled photons is created in the crystal. They are sent to Alice and Bob through 25.3 km of optical fibers. Alice and Bob analyze photons using interferometers equally unbalanced with respect to the pump interferometer. All three interferometers are built using passive 50–50 beam splitters. Alice's and Bob's detection times are also represented.

then through a nonlinear crystal where eventually a pair of photons is created by spontaneous parametric down conversion (SPDC) (see Fig. 1). The state can be written $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - e^{i\varphi}|1\rangle_A|1\rangle_B)$, where $|0\rangle$ represents a photon in the first time bin (having passed through the short arm) and $|1\rangle$ a photon in the second time bin (having passed through the long arm). The index A and B represents Alice and Bob's photon. The phase φ is defined with respect to a reference path length difference between the short and the long arm $\Delta\tau$. The photons A and B are then sent to Alice and Bob who perform projective measurements, by using a similar unbalanced interferometer. There are three detection times on Alice's (Bob's) detectors with the respect to the emission time of the pump laser (see Fig. 1). The first and the last peak (denoted as satellite peaks) corresponds to events which are temporally distinguishable: the left (right) peak corresponds to a photon created in the first (second) time bin which passed through the short (long) arm of Alice's interferometer. When detected in the left (right) satellite peak, the photon is projected onto the vector $|0\rangle$ ($|1\rangle$) (the poles on the Poincaré qubit sphere). Photons detected in the central peak can be either due to events where the created photon is in the first time bin and then it passes through the long arm of Alice's interferometer or due to events where the photon is created in the second time bin and then passes through the short arm of Alice's interferometer. In this case the photon is projected onto the vector $|0\rangle + e^{i\alpha}|1\rangle$ (i.e., on the equator of the Poincaré qubit sphere). Note that when Alice records the central peak she does not observe single photon interference by changing the phase of her interferometer because which-path information can be found by recording the emission time of Bob's photon. With reference to experiments using polarization entangled photons, we refer to this as rotational invariance [13]. If Alice and Bob both record counts in their central peaks, they observe second order interference by changing either the phase in Alice's, in Bob's or in the pump interferometer. The coincidence count rate between Alice and Bob's detectors A_iB_j, is then given by

$$R_{A_i,B_j}(\alpha,\beta,\varphi) \sim 1 + ijV\cos(\alpha+\beta-\varphi) \qquad (1)$$

where i and $j = \pm 1$ (see Fig. 1) and V is visibility of the interference fringes (which can in principle reach the value of 1). We define the imbalance of the pump interferometer as the reference time difference $\Delta\tau$ between the first and the second time bin, the phase φ is thus taken to be zero. The correlation coefficient is defined as

$$E(\alpha,\beta) = \frac{\sum_{i,j} ij R_{A_iB_j}(\alpha,\beta)}{\sum_{i,j} R_{A_iB_j}(\alpha,\beta)} \qquad (2)$$

and by inserting Eq. (1) into Eq. (2) the correlation

coefficient becomes

$$E(\alpha,\beta) = V\cos(\alpha+\beta). \qquad (3)$$

The Bell inequalities define an upper bound for correlations that can be described by local hidden variable theories. One of the most frequently used forms, known as the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality [14], is

$$S = |E(\alpha,\beta) + E(\alpha,\beta') + E(\alpha',\beta') - E(\alpha',\beta)| \leq 2 \qquad (4)$$

Quantum mechanics predicts that S has a maximum value of $S = 2\sqrt{2}$ with $\alpha = 0°, \alpha' = 90°$, $\beta = 45°$, and $\beta' = -45°$. It has been also shown that when the correlation function has sinusoidal form of Eq. (3) and when there is rotational invariance, the boundary condition of Eq. (4) can be written as

$$S = 2\sqrt{2}V \leq 2 \qquad (5)$$

thus $V \geq \frac{1}{\sqrt{2}}$ implies violation of the CHSH Bell inequality, i.e., correlations can not be explained by local hidden variable theories.

Our experimental setup is the following (see Fig. 1): A 150 femtosecond laser pulse with a 710 nm wavelength and with a repetition rate of 75 MHz is first sent through an unbalanced, bulk, Michelson interferometer with an optical path difference of $\Delta\tau = 1.2$ ns and then through a type I LBO (lithium triborate) nonlinear crystal where collinear nondegenerate photon pairs at 1.3 and 1.55 μm wavelength, with bandwidths of around 100 nm, can be created by SPDC. The pump beam is then removed with a silicon filter and the pairs are coupled into an optical fiber. The photons are separated with a wavelength-division-multiplexer, the 1.3 μm photon is sent through 25.3 km of standard optical fiber to Alice having 0.35 dB/km attenuation and the 1.55 μm photon through 25.3 km of dispersion shifted fiber to Bob [15] having 0.25 dB/km of attenuation. Because the created photons have large bandwidths the two time bins will overlap after 25.3 km of optical fibers even when the used optical fibers have zero chromatic dispersion at 1.3 and 1.55 μm, respectively. To avoid this overlap we use interference filters with spectral width of 10 nm for 1.3 μm photons and 18 nm for the 1.55 μm photons. Alice's photon is then measured with a fiber Michelson interferometer and detected by one of two liquid nitrogen cooled passively quenched germanium avalanche photodiodes (APD) A_{+1} or A_{-1}. Their quantum efficiency is of around 10% with 20 kHz of dark counts. In order to select only the central peak events and also to reduce the detector dark counts, a coincidence is made with the emission time of the laser pulse. This signal then triggers Bob's detectors (B_{+1} and B_{-1}) which are two InGaAs APDs (IdQuantique) working in so called gated mode. Although both detectors have similar quantum efficiencies of 20%, one of the detectors (B_{+1}) dark count probability is 2 times smaller than the other one (B_{-1}), and is around 10^{-4}/ns. Using 70 mW of average input

power (measured after the pump interferometer) the probability of creating an entangled qubit per pulse is around 9%. Bob's analyzer is also a Michelson type interferometers built with optical fibers. To better control the phase and to achieve long term stability all three interferometers are passively and actively stabilized. Passive stabilization consists of controlling the temperature of each interferometer. Active stabilization consists of probing the interferometer's phase with a frequency stabilized laser at 1.534 μm (Dicos), and to lock them to a desired value via a feedback loop on a piezoactuator (PZA) included in each interferometer. In order to change path difference in the bulk pump-interferometer, one of the mirrors is mounted on a translation stage including a PZA with the range of around 4 μm. In the analyzing interferometers the long fiber path is wound around a cylindric PZA with a circumference variation range of 60 μm. Contrary to the bulk interferometer which is continuously stabilized, the phase of the fiber interferometers can not be stabilized during the measurement period. Thus we continuously alternate between measurement periods of 100 sec and stabilization periods of 5 sec. This method allows us not only to stabilize the entire setup during several hours, but also to have good control over the changes of both phases α and β.

In order to show a violation of the CHSH Bell inequality after 50 km of optical fibers, we proceed in two steps: first we scan Bob's phase β while Alice's phase α is kept constant. We obtain a raw visibility of around $78 \pm 1.6\%$ (see Fig. 2) from which we can infer an S parameter of $S = 2.206 \pm 0.045$ Eq. (5) leading to a violation of the CHSH Bell inequality by more than 4 standard deviations. The coincidence count rate between any combination of detectors $A_i B_j$ is of around 3 Hz. The raw visibility of the correlation function is mainly reduced due to the creation of multiple pairs (around 9%), due to accidental coincidence counts (related to dark counts of our detectors, around 8%) and due to the misalignment of the interferometers (around 5%). In principle, one could reduce the creation of multiple pairs by reducing the input power, but then the coincidence count rate would also decrease.

With our new interferometers we are able to perform for the first time with time bins the second step: measure the CHSH Bell inequality according to Eq. (4), i.e., lock the phase to the desired value in order to measure the four different correlation coefficients one after the other. To reduce statistical fluctuations, we measure the correlation coefficient Eq. (2) during almost an hour for each setting. The obtained S parameter is $S = 2.185 \pm 0.012$ which shows a violation of the CHSH Bell inequality by more than 15 standard deviations (see Fig. 3).

It has been proven that when the Bell inequality is violated the entangled photons can be used in quantum cryptography [12]. Our QKD protocol is analogous to the Ekert protocol using time-bin entangled photons [16]. Hence, Alice and Bob use two maximally conjugated measurement basis. The first basis is defined by two orthogonal vectors $|0\rangle$ and $|1\rangle$ represented on the poles of the Poincaré qubit sphere (Fig. 1). The projection onto this basis is performed whenever a photon is detected in a satellite peak. Let us illustrate how Alice and Bob encode their bits: whenever Alice detects her photon in the first (second) satellite peak she knows that the pair is created in the first (second) time bin and thus Bob can either detect the twin photon in the first (second) satellite peak or in the central peak, however he can never detect it in the second (first) satellite peak. Thus, after suppressing central peak events with the basis reconciliation, Alice and Bob encode their bits as 0 (1) if the photon is detected in the first (second) satellite peak. The second basis is defined by two orthogonal vectors represented on

FIG. 3 (color online). Correlation coefficients for continuous scan and four different settings. Each data point is derived from a 100 s integration time of coincidence counts between four different combinations of two detectors Eq. (2). As α and β are defined relatively to the pump-interferometer's phase, we use the first three measurement (a), (b), and (c) to define four different phases: $\alpha = 0°$, $\alpha' = 90°$, $\beta = 45°$, and $\beta' = -45°$. The last measurement (d) completes the proof of a violation of the CHSH Bell inequality.
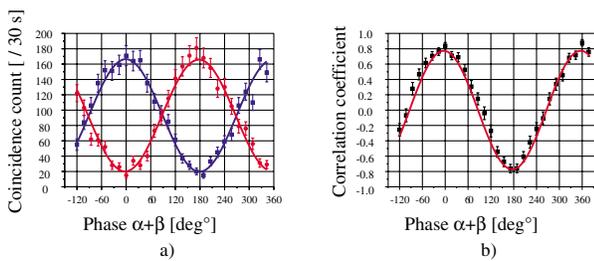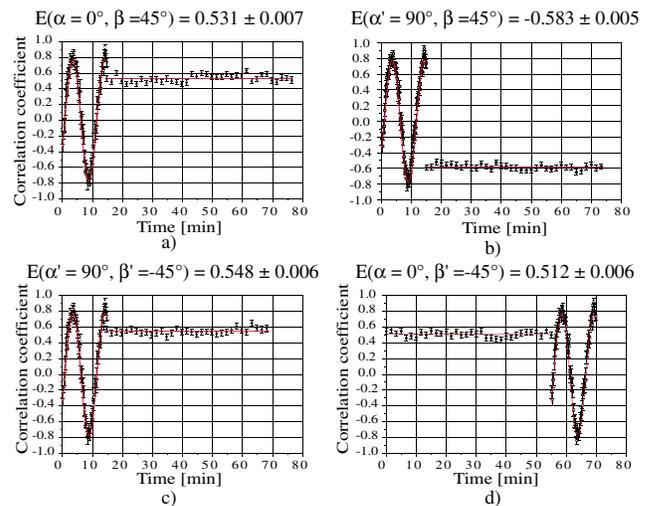

FIG. 2 (color online). (a) Coincidence counts between detectors $A_{+1}B_{+1}$ (circles) and $A_{+1}B_{-1}$ (open squares) (b) Correlation coefficient E(α, β) measured from four different coincidence counts Eq. (2). Alice's phase α is kept constant and Bob's phase β is scanned.

the equator of the Poincaré sphere (for example $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$). The projection onto this basis is performed when a photon is detected in the central peak. Alice and Bob have to correctly adjust their interferometers such that they have perfect correlation between detectors $A_{+1}B_{+1}$ and $A_{-1}B_{-1}$. The encoding of bits 0 and 1 in this basis is thus defined by which detector fires. As Alice and Bob's photon passively choose their respective measurement basis, there is 50% probability that they are detected in the same basis which ensures the security against photon number splitting attack [12].

A proof-of principle of entanglement based QKD over 50 km of optical fiber is performed. In our experimental setup, Alice sequentially selects one of the three detection windows by looking at the arrival time of her photon with respect to the emission of the laser pulse (see Fig. 1). This signal is then used to trigger Bob's detectors. In the first measurement basis the measured quantum bit error rate (QBER) [17] is of $12.8 \pm 0.1\%$ and the measured raw bit rate of around 5 Hz. The QBER is due to accidental coincidence counts (around 8%) and to creation of multiple pairs (around 4.5%). In the second measurement basis the measured QBER is of $10.5 \pm 0.09\%$, with a bit rate of 6 Hz. In this case the QBER is due to accidental coincidence count probability (around 4%), to creation of multiple pairs (around 4.5%) and to slight misalignment of our interferometers (around 2%). In order to have a low statistical error the integration time for both basis is of around six hours. The difference of the QBER measured in two basis is due to the fact that in the first measurement basis the detectors are opened during two time windows instead of one in the second basis. However in the first basis the misalignment of interferometers does not introduce any error. Note that by using two InGaAs APDs with the same low dark count probability as detector B_{+1}, the QBER in the first measurement basis would be reduced to 10.8% and in the second basis to 9.8%. With current detectors, fibers and entangled photons source characteristics the maximal estimated distance to distribute a secrete quantum key is of around 60 km [18].

For a true implementation of QKD using time-bin entangled photons it is necessary that Alice and Bob can monitor detections in all three time windows simultaneously and not, as presented here, one after the other. In addition, as Alice has to trigger Bob's detectors, it is important to ensure that Eve does not get any information about Alice's detection times. This extensions would require more elaborated coincidence electronics but can be easily implemented. Finally, note that Alice's trigger signal has to arrive at Bob's before the photon, thereby putting constraints on the distance between Alice, Bob and the source of entangled photons. The need to wait for the trigger signal could be suppressed by using passively quenched InGaAs APDs or detectors based on superconductivity [19].

In this Letter, we present an experimental distribution of time-bin entangled photons over 50 km of optical fiber. Using active phase stabilization with a frequency stabilized laser and feedback loop, long term stability and control of the interferometer's phase is achieved. In the first experiment, the CHSH Bell inequality is violated by more than 15 standard deviation without removing the detector noise. The possibility of changing the phase in a controlled way allowed us also to show a proof-of-principle of entanglement based QKD over 50 km of optical fiber. An average Quantum Bit Error Rate of 11.5% is demonstrated which is small enough to establish quantum keys secure against individual attacks [20]. Finally, a long term setup stability opens the road for future demonstrations of more complicated quantum communication protocols requiring long measurement times as is the case for the entanglement swapping protocol.

[1] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).
[2] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] C. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (ICCSSP), Bangalore* (IEEE, New York, 1984), p. 175.
[4] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[5] H.-J. Briegle *et al.*, Phys. Rev. Lett. **81**, 5932 (1998).
[6] E. Waks *et al.*, Phys. Rev. A **65**, 052310 (2002); B. C. Jacobs *et al.*, Phys. Rev. A **66**, 052307 (2002); D. Collins *et al.*, quant-ph/0311101 [J. Mod. Opt. (to be published)].
[7] G. Brassard, Found. Phys. **33**, 1593 (2003).
[8] M. Aspelmeyer *et al.*, IEEE J. Sel. Top. Quantum Electron. **9**, 1541 (2003).
[9] M. Aspelmeyer *et al.*, Science **301**, 621 (2003).
[10] J. Brendel *et al.*, Phys. Rev. Lett. **82**, 2594 (1999); R. T. Thew *et al.*, Phys. Rev. A **66**, 062304 (2002).
[11] J. D. Franson, Phys. Rev. Lett. **62**, 2205 (1989); W. Tittel *et al.*, Phys. Rev. Lett. **81**, 3563 (1998).
[12] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002).
[13] J. F. Clauser and M. A. Horn, Phys. Rev. D **10**, 526 (1974).
[14] J. F. Clauser *et al.*, Phys. Rev. Lett. **23**, 880 (1969).
[15] In order to prevent overlapping of different time bins dispersion has to be minimized using dispersion shifted fiber or compensating fibers (see S. Fasel *et al.*, quant-ph/0403144).
[16] W. Tittel *et al.*, Phys. Rev. Lett. **84**, 4737 (2000).
[17] The QBER is defined as the ratio of error rate to total rate.
[18] At larger distances, assuming that Eve can exploit the total QBER with individual attacks, she would get more Shannon information than Bob, hence the secret key rate with one way communication would drop to zero.
[19] R. Sobolewski *et al.*, IEEE Trans. Appl. Supercond., **13**, 1151 (2003).
[20] C. A. Fuchs *et al.*, Phys. Rev. A **56**, 1163 (1997).